FIPS PUB 201

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

(Version 1.0)

Personal Identity Verification (PIV)
for
Federal Employees and Contractors
PUBLIC DRAFT

CATEGORY: INFORMATION SECURITY **SUBCATEGORY: Identification**

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

To be Issued February 25, 2005

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Hratch G. Semerjian, Acting Director

NOTE FOR REVIEWERS

1. Please submit your FIPS 201 and Special Publication 800-73 comments using the comment template form provided. Please include the submitter's name and organization in the header section of the spreadsheet. This will greatly facilitate processing of comments by NIST.

2. Comments should be submitted to DraftFips201@nist.gov. It is requested that Federal organizations submit one consolidated/coordinated set of comments. Also, include "Comments on Public Draft FIPS 201" in the subject line.

3. The comment period closes at 5:00 EST (US and Canada) on December 23, 2004. Comments received after the comment period closes will be handled on as-time-is-available basis.

4. Please note that the Public Draft of FIPS 201 contains two major sections. Part 1 includes control objectives derived from HSPD #12 and an identity proofing process structured to satisfy the intent of HSPD #12 and provide for reciprocity. Part 2 includes detailed specifications intended to support technical interoperability among Federal departments and agencies.

FOREWORD

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act of 2002 (FISMA).

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

Dr. Shashi Phoha, Director
Information Technology Laboratory

ABSTRACT

This standard specifies an architecture and technical requirements for a common identification standard for Federal employees and contractors. The standard addresses several problems requiring reliable and cost effective solutions in personal identification as it applies to access control. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of an individual seeking physical access to Federally-controlled Government facilities and electronic access to Government information systems. The standard identifies the problems to be solved, defines a common identity verification architecture, and describes the components, interfaces, support services, and life-cycle management functions needed to achieve requisite levels of security assurance for applications that require different levels of protection. The standard also incorporates and refers to other technical and operational standards necessary to achieve interoperability among identification cards, electronic card readers, communication systems, and access control systems interfaces.

Keywords: Architecture, authentication, authorization, biometrics, credential, cryptography, identification, identity, infrastructure, Federal Information Processing Standard (FIPS), model, validation, verification.

Federal Information Standards Processing 201

2005

Announcing the

Personal Identity Verification
for
Federal Employees and Contractors

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to the Federal Information Security Act of 2002.

1. Name of Standard.

FIPS PUB 201: Personal Identity Verification (PIV) for Federal Employees and Contractors

2. Category of Standard.

Information Security.

3. Explanation.

Homeland Security Presidential Directive (HSPD) 12, dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors," directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. It further specified secure and reliable identification that:

- Is issued based on sound criteria for verifying an individual employee's identity;
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Can be rapidly authenticated electronically; and
- Is issued only by providers whose reliability has been established by an official accreditation process.

The directive stipulated that the standard include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. As promptly as possible, but in no case later than eight (8) months after the date of promulgation, executive departments and agencies are required to use the standard for identification issued to Federal employees and contractors in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems.

This standard is comprised of two parts, hereafter referred to as PIV-I and PIV-II. PIV-I, describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of the HSPD-12, including the personal identity proofing process, but does not address the interoperability of PIV cards and systems among agencies. PIV-II provides detailed technical specifications to support control and security objectives in PIV-I. Specifically, PIV-II provides details for technical interoperability of Personal Identity Verification (PIV) cards with the personal authentication, access control, and PIV card

management systems across the Federal Government. This standard does not specify access control policies for agencies.

4. Approving Authority.

Secretary of Commerce.

5. Maintenance Agency.

Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).

6. Applicability.

This standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems except for "national security systems" as defined by FISMA. Except as provided in HSPD-12, nothing in this standard alters the ability of government or non-government entities to utilize the standard for additional applications.

7. Specifications.

Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) Standard (affixed).

8. Implementations.

The PIV standard is comprised of two parts: PIV-I and PIV-II. PIV-I meets the control objective and security requirements of HSPD-12, while PIV-II meets the technical interoperability requirements of HSPD-12. PIV-II specifies the technical details to enable agencies to implement and use interoperable and secure identity credentials in a Federal personal identity verification system.

PIV cards must be personalized with identity information for the individual to whom the card is issued, for identity verification both by humans and automated systems. Humans can use the physical card for visual comparisons, while systems can use the electronically stored data on the card to conduct automated identity verification.

Graduated position sensitivity levels identified in the standard apply to identity source document proofing and registration as part of the issuance process. To help ensure reliability, agencies accredit issuers who issue identity credentials to their employees and contractors until a Government-wide PIV-II accreditation process is established.

The standard also covers security and interoperability requirements for PIV cards. Funding permitting, NIST plans to develop a PIV Validation Program that will test implementations for conformance with this standard. Information on this program will be published at http://csrc.nist.gov/PIV-Project/Conformance/ as it becomes available.

9. Effective Date.

This standard becomes effective February 25, 2005. Agencies shall meet the requirements of PIV-I no later than October 2005, in accordance with the timetable specified in HSPD-12.

Office of Management and Budget (OMB) has advised NIST that it plans to issue guidance regarding agency development of transition plans to PIV-II.

10. Qualifications.

The security provided by the PIV system is dependent on many factors outside the scope of this standard. Organizations adopting this standard must be aware that the overall security of the personal identification system relies on the:

- Assurance provided by the parent organization that the person to be issued the credential has been correctly identified;
- Position sensitivity levels selected by the PIV card issuer;
- Protection provided to identity verification data stored within the PIV card and transmitted between the card and the PIV issuance and usage infrastructure; and
- Protection provided to the identity verification system infrastructure and components throughout the entire life cycle.

While it is the intent of this standard to specify mechanisms and support systems that provide high assurance personal identity verification, conformance to this standard does not assure that a particular implementation is secure. It is the responsibility of Federal departments and agencies to ensure that components, interfaces, communications, storage media, managerial processes, and services used within the identity verification system are designed and built in a secure manner.

Similarly, the use of a product that conforms to this standard does not guarantee the security of the overall system in which the product is used. The responsible authority in each agency shall assure that an overall system provides the acceptable level of security.

Since a standard of this nature must be flexible enough to adapt to advancements and innovations in science and technology, the maintenance agency will review this standard every five years to assess its adequacy.

11. Waivers.

As per the Federal Information Systems Management Act of 2002, waivers to Federal Information Processing Standards are no longer allowed.

12. Where to obtain copies.

This publication is available through the Internet by accessing http://csrc.nist.gov/publications/.

Federal Information Processing Standards Publication 201
Specifications for
Personal Identity Verification

TABLE OF CONTENT

TABLE OF FIGURES

Title **Page Number**

LIST OF TABLES

Title **Page Number**

[This page intentionally left blank.]

1 INTRODUCTION

Authentication of an individual's identity is a fundamental component of physical and computer access control processes. When individuals attempt to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of identity is needed to make sound access control decisions.

A wide range of mechanisms is employed to authenticate identity, leveraging many different classes of identification identity credentials. For physical access, individual identity has traditionally been authenticated by use of paper credentials, such as driver's licenses and badges. Access to computers and data has traditionally been authenticated through user-selected passwords. More recently, cryptographic mechanisms and biometric techniques have been applied to physical and computer security, replacing or supplementing the traditional credentials.

The strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential. This document establishes a standard for personal identity verification based on secure and reliable forms of identification credentials issued by the Federal Government to its employees and contractors. These credentials are intended to authenticate individuals that require access to Federally-controlled facilities, information systems, and applications. This standard addresses requirements for identity proofing, infrastructures to support interoperability of identity credentials, and validation and accreditation of applications and processes. Additionally, this standard provides technical mechanisms to support authentication for both physical and logical access. However, this standard does not specify physical and logical access control mechanisms and processes.

1.1 Purpose

The purpose of this standard is to develop a reliable Government-wide Personal Identity Verification (PIV) system for use in applications such as access to Federally-controlled facilities and information systems. This standard has been developed within the context and constraints of Federal policy and information processing technology currently available and evolving.

This standard defines requirements for a PIV system within which common identification credentials can be established and shared. The standard also identifies Federal Government-wide requirements for security levels that are dependent on risks to the facility or information being protected.

1.2 Scope

Homeland Security Presidential Directive 12 (HSPD-12), signed by the President on August 27 2004, established the requirements for a common identification standard for identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information system. HSPD-12 directs the Department of Commerce to develop a Federal Information Processing Standard (FIPS) to define such common identification credential. In accordance with the HSPD-12, this standard defines the technical requirements for the identity credential that is:

- Issued based on sound criteria for verifying an individual employee's identity;
- Resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Rapidly authenticated electronically; and
- Issued only by providers whose reliability has been established by an official accreditation process.

Additionally, this standard defines graduated position sensitivity levels for purposes of identity credential issuance and source document proofing. The standard also defines authentication mechanisms offering varying degrees of security. Note that the Federal departments and agencies must determine the position sensitivity level required for their employees / contractors and authentication mechanisms appropriate for their applications. Therefore, the scope of this standard is limited to authentication of an individual's identity. Access authorization decisions are outside the scope of this standard.

1.3 Document Organization

This standard is composed of two parts, PIV-I and PIV-II. The first part (PIV-I) describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of the HSPD-12, including the personal identity proofing process but does not address the interoperability of PIV cards and systems among agencies. The second part (PIV-II) provides detailed technical specifications to support control and security objectives in PIV-I. Specifically, PIV-II provides details for technical interoperability of PIV cards with the personal authentication, access control, and PIV card management systems across the Federal Government.

Implementers of the standard should note that Sections 1, 3, and 6 of this document are *informative*, and serve to provide critical background information for understanding the PIV standard. Section 6 provides guidance on wide range authentication mechanisms. This standard does not restrict the agencies from adopting additional alternatives. Section 2 of the standard is *normative*, and provides the requirements for the first part (PIV-I) of the standard, by establishing the control and security objectives for compliance with HSPD-12. Sections 4 and 5, and all appendices, unless otherwise stated, are *normative* and contain language that is to be followed literally and explicitly in order for a given implementation to be deemed compliant with the second part (PIV-II) of the standard which facilitates a fully interoperable PIV system across the Federal Government.

PART 1: PIV-I

This part describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of the HSPD-12, including the personal identity proofing process.

Implementation Timeframe: In accordance with HSPD-12, agencies shall meet the requirements of this part no later than October 2005.

2 COMMON IDENTIFICATION AND SECURITY REQUIREMENTS

This section provides the requirements for the first part of the PIV standard. PIV-I addresses the fundamental control objectives and security objectives outlined in HSPD-12, including the personal identity proofing process for new employees, but does not address interoperability of PIV cards and systems among agencies or compel the use of a single, universal credential.

2.1 Control Objectives

HSPD-12 established control objectives for secure and reliable identification of Federal employees and contractors. Based on this directive, agency Personal Identity Verification Systems shall:

- Use the Government-wide identity proofing and registration process defined in Section 2.2;
- Use the Government-wide identity credential issuance process defined in Section 2.3;
- Issue credentials through systems and providers whose reliability has been established by the agency and so documented and approved in writing;
- Issue identity credentials that are resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Implement an identity credentialing system that supports rapid electronic authentication of Federal employees and contractors; and
- Support credentials for physical and logical access to Federally controlled facilities and information systems.

In PIV-II these identity proofing and issuance requirements are maintained, and a common Government-wide, interoperable PIV card is required. This common PIV card supports the control objectives listed above and, with the Government-wide credential issuance process and issuer Certification and Accreditation already established in PIV-I, allows agencies to both trust and use the PIV credentials of other agencies, for physical and logical access control.

2.2 Identity Proofing and Registration Process

For compliance to the PIV-I control objective 1, at a minimum, agencies shall follow the identity proofing and registration process defined in Sections 2.2.1- 2.2.4 when issuing identity credentials. It should be noted that one individual shall not assume more than one role in this process. The critical *roles* associated with the PIV identity proofing and issuance process are:

- Applicant — the individual to whom an identity credential needs to be issued;
- PIV Requesting Official — The individual who initiates a request for an identity credential on behalf of an Applicant;

- PIV Authorizing Official — The individual who approves the request for an identity credential;
- PIV Registration Authority — The entity that performs the identity proofing and background checks;
- PIV Issuing Authority — The entity that issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed.

2.2.1 Identity Proofing and Registration of New Employees and Contractors

The paper-based source documents by themselves provide very weak assurance of identity. The process described in this section supplements document inspection with background checks designed to improve assurance of identity.

An Applicant applies for an identity credential as a part of the vetting process for Federal employment. An Applicant provides two forms of identification from the list of acceptable documents included in the *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification* to the PIV Registration Authority. At least, one of the documents shall be a valid State or Federal Government-issued picture ID. The PIV Requesting Official shall submit the PIV request and photocopies of identity source documents for the Applicant to the PIV Authorizing Official. The PIV Authorizing Official shall approve the request and forward it together with photocopies of the identity source documents to the Registration Authority and the PIV Issuing Authority. The PIV request shall include:

- Name, organization, and contact information of the PIV Requesting Official;
- Name, date of birth, position including the position sensitivity level, and contact information of the Applicant including address of Applicant's parent organization;
- Name, organization, and contact information of the PIV Authorizing Official;
- Name and contact information of the Registration Authority;
- Name and contact information of the Issuing Authority; and
- Signatures of the Requesting and the Authorizing Officials.

Based on the required position sensitivity level, the Applicant shall complete the appropriate background information form listed Table 2-1.

Table 2-1: Background Information Forms Required from Applicant

Position Sensitivity Level	Form
1	Form I-9, OMB No. 1115-0136, Employment Eligibility Verification
2	Standard Form 85, OPM Questionnaire for Non-sensitive Positions or equivalent
3	Standard Form 85 P, OPM Questionnaire for Public Trust Positions or equivalent
4	Standard Form 85 P, OPM Questionnaire for Public Trust Positions or equivalent

The Applicant shall provide the completed background information form to the Registration Authority. In addition, the Applicant shall appear in person and provide two forms of identity source documents provided earlier to the PIV Requesting Official. The Registration Authority shall visually inspect the identification documents and authenticate them as being acceptable. The Registration Authority shall subsequently compare the picture on the source document to the Applicant to confirm the Applicant is the holder of the identity source document. Additionally, the Registration Authority shall compare the Applicant information contained in the PIV request (such as full name, date of birth, and contact information) with the corresponding information provided by the Applicant. At this time, the Registration Authority shall fingerprint the Applicant by collecting all of the Applicant's fingerprints as defined in Section 4.4.3.

The Registration Authority shall conduct the appropriate background check as defined in Table 2-2 using the position sensitivity level from the PIV Request for the Applicant. After successful completion of the appropriate background check, the Registration Authority shall notify the Issuing Authority that an identity credential can be issued to the Applicant.

Table 2-2: Background Checks By Position Sensitivity Level

Position Sensitivity Level	Personal Identity Background Checks
1 Low	Authentication of Applicant Identity Source Documents conducted by entity responsible for authorizing PIV card issuance (checking and verifying validity with each Document's Issuer). Law enforcement check (fingerprint).
2 Moderate	National Agency Check and Inquiries (NACI). Refer to Annex D for additional details.
3 High	NACI and Credit Check (NACIC). Refer to Annex D for additional details.
4 Critical (Vital National Asset-Critical Infrastructure)	Limited Background (LBI) or Background Investigation (BI). Refer to Annex D for additional details.

The Registration Authority shall be responsible to maintain:

- Completed and signed PIV request,
- Copies of the identity source documents,
- Completed and signed background form received from the Applicant,
- Results of the required background check, and
- Any other materials used to prove the identity of the Applicant.

2.2.2 Identity Proofing and Registration of Current Employees

When issuing or re-issuing identity credentials to current employees, the identity proofing (including the application and approval process) described in Section 2.2.1 shall be followed except that background checks are not required if the results of the most recent previous check are on-file and can be referenced in the application process and verified by the Registration Authority.

2.2.3 Access Pending Identity Proofing

Until the required credential verification or background investigation is complete, employees and contractors shall not be issued long-tem identity credentials but shall be treated according to visitor procedures.

2.2.4 Identity Proofing and Registration of Overseas Foreign Workers

For citizens of foreign countries who are working for the U.S. Federal Government overseas, a similar process (See Section 2.2.1) for registration and approval shall be established using a method approved by the U.S. Department of State Bureau of Diplomatic Security.

2.3 Identity Credential Issuance

The Issuing Authority shall confirm the validity of the PIV request received from the PIV Authorizing Official and the notification received from the Registration Authority. The Applicant shall appear in person to the Issuing Authority and present the original identity source documents. Before issuing the identity credential, the Issuing Authority shall verify that the individual who collects the identity credential is indeed the Applicant. (I.e., the Issuing Authority shall compare the Applicant to the original identity source documents and ensure that the photocopies received from the Authorizing Official match.) The Issuing Authority shall photograph the Applicant at the time of issuance and retain a file copy of the image. The identity credential shall then be personalized for the Applicant.

The Issuing Authority shall be responsible to maintain:

- Completed and formally authorized PIV Request.
- The name of the PIV identity credential holder (Applicant).

- The credential identifier such as an identity credential serial number.
- The expiration date of the identity credential.

.

PART 2: PIV-II

This part provides detailed technical specifications of components and processes for interoperability of PIV cards with the personal authentication, access control, and PIV card management systems across the Federal Government.

Implementation Timeframe: OMB has advised NIST that it plans to issue guidance regarding agency development of transition plans to part 2.

3 PIV SYSTEM OVERVIEW

The PIV system is comprised of components and processes that support a common (smart card based) platform for identity authentication across Federal agencies, and across multiple types of physical and logical access environments.

The component specifications contained in this standard promote uniformity and interoperability amongst the various PIV system components, and across agencies and installations. The process specifications contained in this standard serve as a set of minimum requirements for the various activities that need to be performed within an operational PIV System.

When implemented in accordance with this standard, the PIV card supports a set of position sensitivity levels and a suite of identity authentication mechanisms that can be used across agencies in a consistent manner. The authenticated identity information can then be used as a basis for access control in a variety of Federal physical and logical access environments.

The following sections briefly discuss PIV system objectives, roles and responsibilities, components and their usage, and lifecycle activities of the PIV card.

3.1 Functional Objectives

The goal of the PIV system is to provide for a secure and reliable form of Federal employee and contractor identification. This will address the disparities in the quality and security of forms of identification currently used to gain access to Federal facilities. Some of the threats to the current systems include the following:

- Improper issuance of a valid card.
- Use of a stolen or borrowed card to gain access.
- Production of counterfeit cards.
- Use of lower sensitivity cards to gain access to more sensitive and critical assets.

The following objectives are used to mitigate these threats and guide the development of this standard.

- Collect and evaluate information sufficient to assure that the legal identity claimed by a PIV Applicant is accurate;
- Provide a PIV card that may subsequently be used to verify the cardholder (an Applicant who is issued a PIV card) identity rapidly and securely;
- Protect the privacy of the cardholder;

- Specify interfaces necessary to read the PIV card efficiently wherever offered by the cardholder when requesting access;
- Provide appropriate security to the entire identity proofing and authentication process;
- Provide protection against use of cloned or counterfeited PIV cards;
- Provide adequate security technology, management procedures, and services to protect the PIV system from being circumvented; and
- Support interoperability so that PIV cardholders may be authenticated by any Government facility or information system, regardless of the cardholder's parent organization.

3.2 PIV Responsibilities

Since the PIV system is composed of components and processes across Federal departments and agencies, all entities involved in identity management play a critical role. This section defines some high-level roles in the system and assigns responsibility to each of them.

3.2.1 Agency Responsibilities

Federal departments and agencies that issue and use identity credentials will be responsible for:

- Establishing position sensitivity levels for Applicants;
- Authenticating and vetting Applicants for PIV cards;
- Issuing PIV cards to approved Applicants;
- Authorizing PIV cardholders access to physical facilities and information systems;
- Maintaining records of registration and PIV card status information;
- Operating and maintaining their portion of the PIV system to assure the objectives of this standard; and
- Cooperating with other agencies in using the PIV system to control and grant access to all people authorized at the level required by the facility or information system.

3.2.2 Applicant Responsibilities

Applicants are responsible for:

- Providing authentic identity source documents when requested,

- Completing accurately all position and PIV application forms, and
- Cooperating in the PIV applicant vetting process and providing biometrics as needed.

3.2.3 Oversight Responsibilities

Certain agencies have specific responsibilities for implementing this standard:

- NIST is responsible for establishing standards, recommendations, guidelines, and conformance tests for components of the PIV system.
- OMB is responsible for reviewing and approving PIV system budgets and operational procedures.
- GSA is responsible for assisting agencies to procure and operate PIV sub-systems.
- OPM is responsible for assisting agencies to authenticate and vet applicants in accordance with relevant laws and executive orders.

3.3 Functional Components

An operational PIV System can be logically divided into the following two major subsystems:

- ***PIV System Front-End Subsystem*** — the PIV card, card and biometric readers, and the PIN Pad device. The PIV cardholder interacts with these components in order to gain physical or logical access to the desired Federal resource.
- ***PIV Card Issuance and Management Subsystem*** — the components responsible for identity proofing and registration, card issuance and key management, as well as the various repositories and services (PKI credentials, certificate status servers etc) required as part of the verification infrastructure.

There is another subsystem that becomes relevant when the PIV card is used to authenticate a cardholder who is seeking access to a physical or logical resource. Although this subsystem does not fall within the scope of the standard, various mechanisms for identification and authentication have been discussed within the standard in order to provide consistent and secure means for performing these functions.

- ***Access Control Subsystem*** — the physical and logical access control systems, the protected resources, and the authorization data.

The Figure 3-1 illustrates the functional model for the operational PIV system, identifying the various system components and the direction of data flow between these components.

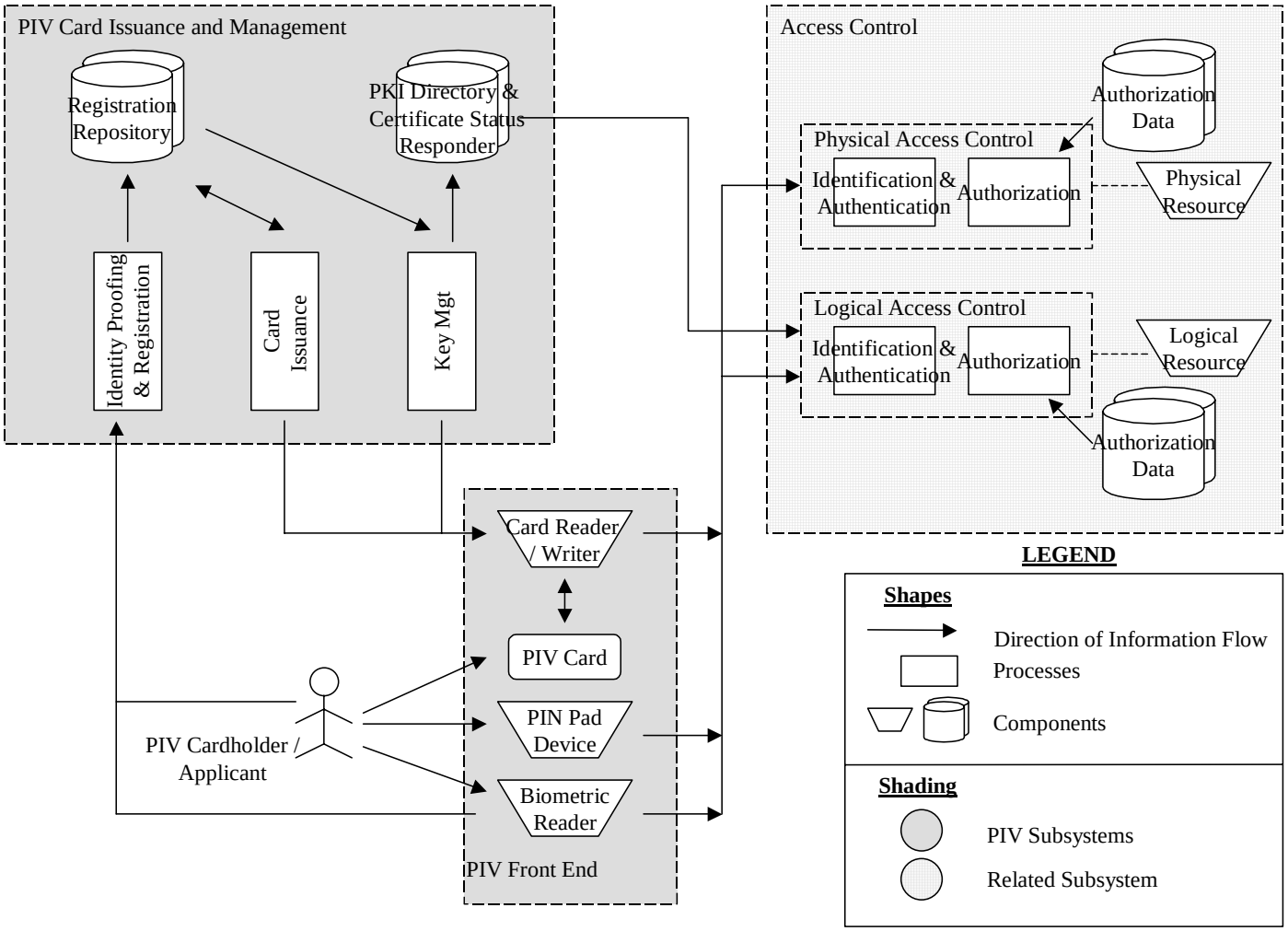


FIGURE 3-1: PIV SYSTEM FUNCTIONAL MODEL

3.3.1 PIV Front-End Subsystem

The PIV card is issued to the Applicant upon completion of all registration processes. This PIV card has a "credit card" sized form factor, with one or more embedded integrated circuit chips (ICC) that provide memory capacity as well as computational capability. This PIV card is the primary component of the PIV system and is used by its holder for authentication to various physical and logical resources.

Card readers are located at access points for controlled resources where a cardholder may wish to gain access (both physical and logical) by using the PIV card. The reader communicates with the PIV card to retrieve the appropriate information, located in the memory of the card, in order to pass it to the access control systems for granting or denying access.

Card writers are very similar to the card readers and are used for personalization and initialization of the information that needs to be stored on PIV cards. The data to be stored on PIV cards include personal information, certificates, the Personal Identification Number (PIN), biometric data and is discussed in further detail in later sections.

Similar to the card reader, the biometric reader may be located at secure locations where a cardholder may wish to gain access by using the PIV card. Biometric readers depend upon the use of stored biometric data of the cardholder, stored in the memory of the card, and it's comparison of a real-time biometric sample. The use of biometrics provides an additional factor of authentication (something you are[1]), in addition to providing the card (something you have).

As with a biometric reader, a PIN pad device can also be used along with the card readers at secure locations where a higher level of authentication assurance of the cardholder is required. The cardholder presenting the PIV card must type in their PIN into the PIN pad. The PIN pad therefore also supports the use of an additional factor of authentication (something you know), in addition to providing the card (something you have) to provide a higher level of authentication assurance.

3.3.2 PIV Card Issuance and Management Subsystem

The Identity Proofing and Registration component in Figure 3-1 refers to process of collection, storage, and maintenance of all information and documentation that is required to authenticate and assure the identity of the applicant. Information such as the full name, address, date of birth, marital status, Federal designation, sponsor identity, and biometric information, are examples of information collected from the Applicant at the time of registration.

All of the Applicant registration data collected at the onset of the registration process including the biometric data, as well any updates to this information during the usage of this card, is stored in the Registration Repository.

The security mechanisms available on a PIV card may be used in a challenge response protocol to verify the authenticity of the card and the cardholder. The generation of the key pairs, distribution of digital certificates containing the public key of the cardholder, management of the

[1] *For more information on the terms "something you know," "something you have," and "something you are," see [SP800-63].*

certificates so that application can be prohibited from using certificates which are no longer valid, are all part of Key Management component. This Key Management component are used throughout the lifecycle of PIV cards from issuance of Public Key Infrastructure (PKI) credentials, to usage of PKI credentials for secure operations, to eventual re-issuance or termination of the card. Key management is also responsible for the provisioning of publicly accessible repositories and services (such as the PKI repository) that inform the requesting application on the status of these PKI credentials.

The Card Issuance component primarily deals with the personalization of the physical (visual surface) and logical (contents of ICC) aspects of the card. This includes printing of photographs, name and other information on the card as well as loading the relevant card applications, biometrics, and other data. The PIN to unlock the card may also be collected from the Applicant or generated at the time of issuance, and embedded within the PIV card.

3.3.3 PIV Access Control Subsystem

Physical and logical resources are the end targets of the entire PIV system. A physical resource is the secured facility (building entrances, rooms, turnstiles, parking gates, etc.) that the cardholder desires to access. The logical resource is typically a location on the network (e.g., computer workstations, folders, files, database records, or software programs) to which the cardholder desires to gain access.

The authorization data component for both the physical and logical resource is populated with relevant cardholder access information. An example of this can be a simple Access Control List (ACL).

The physical and logical access control system grants or denies access to a particular resource and includes an Identification and Authentication (I&A) component as well as an authorization component. The I&A component interacts with the PIV card and uses mechanisms discussed in Section 6 to identify and authenticate cardholders. Once authenticated, the authorization component interacts with the authorization data component to match the cardholder provided information to the information on record. The access control components typically interface with the card reader, the authorization data, PIN pad device, certificate status services, and optionally with the biometric reader.

3.4 Card Lifecycle Activities

The PIV card lifecycle primarily consists of seven activities. The activities that take place during fabrication and pre-personalization of the card at the manufacturers are not considered a part of this lifecycle model. Figure 3-2 presents these PIV activities and shows the PIV card request as the initial activity and PIV card termination as the end of life.

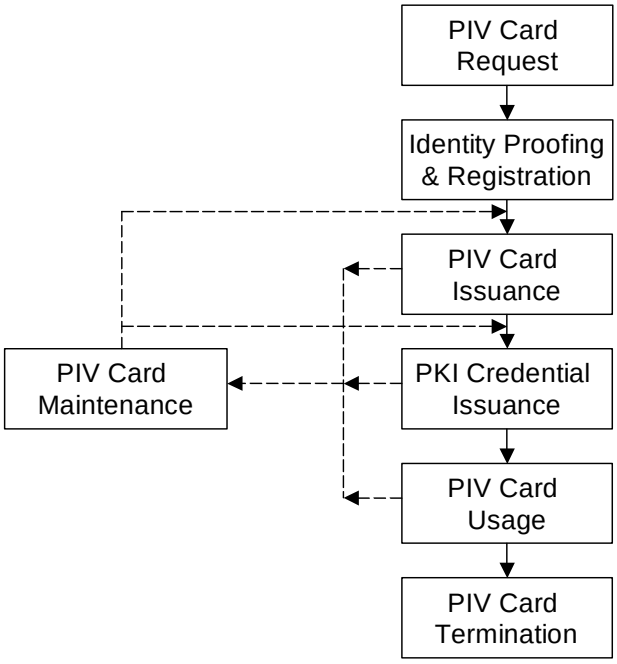


FIGURE 3-2: PIV CARD LIFECYCLE ACTIVITIES

- ***PIV card request*** — This activity deals with the initiation of a request for the issuance of a PIV card to an applicant by the PIV Requesting Official as well as the validation of this request by the PIV Authorizing Official.

- ***Identity proofing and registration*** — The goal of this activity is to verify claimed identity of the Applicant and that the entire set of identity source documents presented at the time of registration is valid. On successful validation of these documents, the Applicant is enrolled into the agency's PIV Management System.

- ***PIV card issuance*** — This activity primarily deals with the personalization (physical and logical) of the card and the issuance of the card to the intended Applicant.

- ***PKI credential issuance*** — This activity deals with generation of logical credentials and loading them onto the PIV card.

- ***PIV card usage*** — The main purpose of issuing a PIV card is so that a cardholder can be authenticated or verified at a later point in time before providing physical or logical access. Access authorization decisions can then be made once the cardholder is successfully authenticated as part of this phase.

- ***PIV card maintenance*** — This activity deals with the maintenance or update of the physical card as well as the data such as various card applications, PIN, PKI credentials, and biometrics stored on it.

- ***PIV card termination*** — The termination process is used to permanently destroy or invalidate the usage of the card including the data on it including the keys such that it cannot be used again.

4 FRONT-END SUBSYSTEM

This section identifies the requirements for the components of the PIV system. The requirements for PIV card layout, card data objects, card reader, and biometrics are provided below.

Section 4.1 provides the physical and logical card specifications. The PIV Cardholder Unique Identification (CHUID) object is described in Section 4.2. Cryptographic keys associated with the cardholder are described in Section 4.3. Formats for mandatory biometric information is defined in Section 4.4.

4.1 PIV Card Specifications

Sections 4.1.1 – 4.1.3 provides a description of applicable standards, tamper proofing requirements, and physical characteristics of the PIV card. Section 4.1.4 describes the card topography. Section 4.1.5 provides the PIV card data storage requirements. Finally, activation of logical credentials on a PIV card is described in Section 4.1.6.

The side of the card that contains the contacts is referred to as the front of the card and the other side is referred to as the back of the card. The PIV card shall comply with physical characteristics as delineated in ISO/IEC 7810, ISO/IEC 10373, ISO/IEC 7816 for contact cards, and ISO/IEC 14443 for contactless cards. The PIV card shall comply with [ANSI322] as stated in the Section 4.1.3. Any manufacturing process required to meet the requirements in the standard shall meet the specified standards and shall result in a flat card.

4.1.1 Printed Material

4.1.1.a. The printing shall not rub off during the life of the PIV card nor deposit debris on the plastic card printer rollers during printing and laminating.

4.1.1.b. Printed material shall not interfere with contact and contactless placement or impede access to the contents therein.

4.1.2 Physical Security Tamper Proofing and Resistance

4.1.2.a. A tri-modal or bi-modal optical variable device (OVD) or optical variable ink (OVI) shall be embedded in the card material on the front of the card. The OVD or OVI shall be such that it is transparent when looking at it directly and changes colors as the viewing angle changes. Incorporation of this feature within the card body shall be free of defects, such as fading, discoloration, or contamination as determined by a visual inspection.

4.1.2.b. Additional tamper resistance and anti-counterfeiting methods may be incorporated at an agency's discretion. Federal agencies are strongly encouraged to review the viability, effectiveness, and currency of these tamper resistance and anti-counterfeiting methods.

4.1.3 Physical Characteristics and Durability

4.1.3.a. The PIV card shall contain a contact and contactless ICC interface.

4.1.3.b. The card body shall be a polyvinyl chloride (PVC) PVC core with polyethylene terephthalate (PET) layers or a similar card material type satisfying the durability requirements specified in [ANSI 322] and ISO/IEC 7810.

4.1.3.c. The card shall be 27 to 33 mil card thickness (prior to lamination) in accordance with ISO/IEC 7810.

4.1.3.d. The cards shall be subjected to [ANSI322]. While the [ANSI322] test methods do not currently specify compliance requirements, the tests shall be used to compare card durability and performance. The [ANSI322] tests minimally shall include; card flexure, static stress, plasticizer exposure, impact resistance, card structural integrity, surface abrasion, temperature and humidity induced dye migration, ultraviolet light exposure, a laundry test and optionally magnetic stripe abrasion.

4.1.3.e. At the agency's discretion, the card may be required to be resistant to chemical effects arising from use in a flight line or equally austere environment.

4.1.3.f. The PIV card shall not be embossed.

4.1.3.g. The PIV card shall not be punched with holes or physically altered in any similar fashion.

4.1.3.h. Decals shall not be adhered to the card.

4.1.3.i. The cardstock shall withstand the effects of high temperatures required by the application of a polyester laminate on one or both sides of the card by commercial, off-the-shelf (COTS) equipment. The cardstock provided shall allow production of a flat card in accordance with [ISO7810] after lamination of one or both sides of the card.

4.1.3.j. Cards shall not malfunction or delaminate after hand cleaning with a mild soap and water. The reagents called out in Section 5.4.1.1 of [ISO10373] shall be modified to include a 2% soap solution. A card shall be deemed acceptable if it meets these cleaning requirements

4.1.3.k. The card shall be subjected to actual, concentrated or artificial sunlight to appropriately reflect 2000 hours of Southwestern United States sunlight exposure in accordance with Section 5.12 of [ISO10373]. Concentrated sunlight exposure shall be performed in accordance with [G90-98], and accelerated exposure in accordance with [G155-00]. After exposure, the card shall be subjected to the [ISO10373] dynamic bending test and shall have no visible cracks or failures. Alternatively, the card may be subjected to the [ANSI322] tests for ultraviolet and daylight fading resistance and subject to the same [ISO10373] dynamic bending test.

4.1.3.l. In the case that OVDs are used as a tamper resistant feature, the minimum peel strength requirement in [ISO7810] may not be met for the OVD patch in the layer of the cardstock that contains it and as such the minimum peel strength requirement shall be addressed on a case-by-case basis. However, the remainder of the cardstock layer with the OVD and the remainder of the card body shall meet all requirements of [ISO7810].

4.1.4 Topography Requirements

The information on a PIV card shall be in both visual and electronic form. This section does not cover information stored in the ICCs. This standard does not specify whether a single chip or multiple chips are used to support the mandated contact and contactless interfaces.

4.1.4.1 Front of the Card (Mandatory)
A pictorial representation of the mandatory and optional visual information on the front of the card is provided in Figure 4-1. The placement of Zones shall be printed on the card as designated. Figure 4-1 is not to scale.

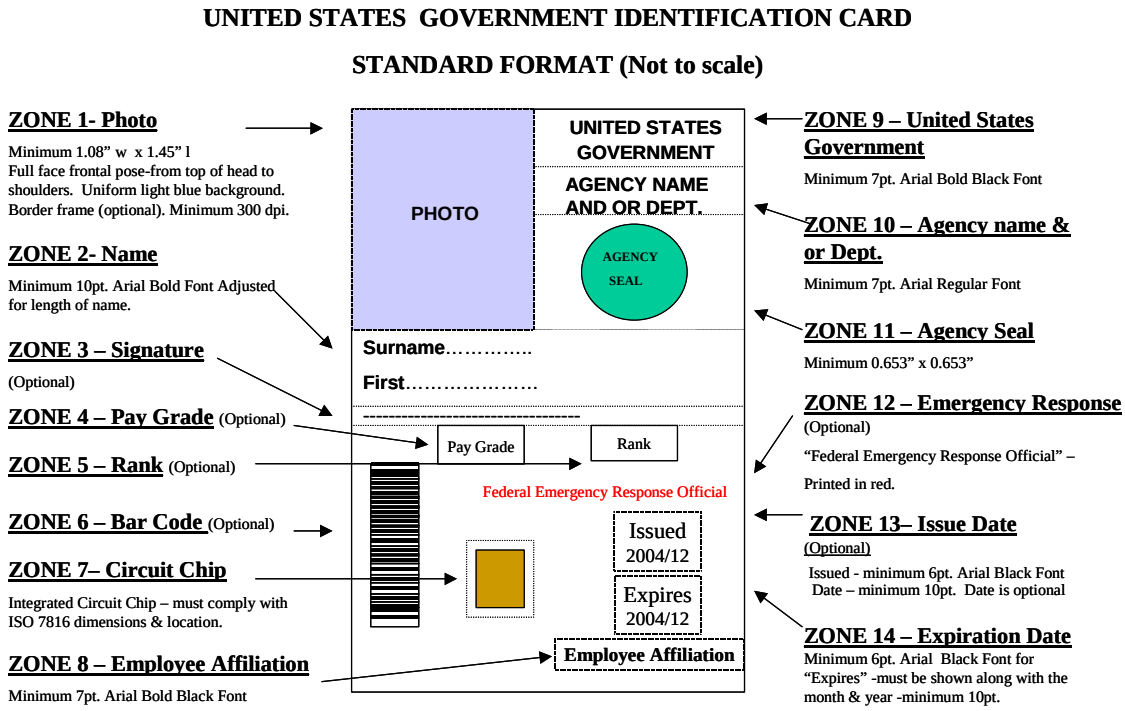


FIGURE 4-1: FRONT OF THE PIV CARD

The description of each mandatory information item follows.

4.1.4.1.a. Zone 1 – Photograph. The photograph shall be placed in the upper left corner. The photo will be placed such that it does not conflict with contact or contactless chip placement. The photograph shall be a full frontal pose from top of the head to shoulder. The minimum size shall be 1.08 inch wide and 1.45 inch in length although larger photos will better facilitate visual verification. A minimum of 300 dpi resolution shall be required. A photo border frame is optional.

4.1.4.1.b. Zone 2 – Name. The surname and first names shall be printed under the photograph in capital letters in the order depicted. The font shall be Arial Bold of minimum 10pt size.

4.1.4.1.c. Zone 8 - Employee Affiliation Employment Identifier. The employee affiliation, such as "CONTRACTOR," "ACTIVE DUTY", "CIVILIAN" or an Agency-specific employee identifier or nomenclature, shall be printed in the Arial Bold Black font of minimum 7pt size.

4.1.4.1.d. Zone 9 - Text "United States Government". The "UNITED STATES GOVERNMENT" text shall be printed on the top front portion of the card and shall be capitalized in the Arial Bold Black font of minimum 7 pt size.

4.1.4.1.e. Zone 14 - Expiration Date. The card expiration date shall be printed in the lower right hand corner of the card in the ISO/IEC 8601 format YYYY/MM. The font for the text "Expires" shall be Arial Black of minimum 6 pt size. The font for date shall be Arial Black of minimum 10pt size.

4.1.4.2 Back of the Card (Mandatory)

The pictorial representation of the mandatory visual information on the back of the card is provided in Figure 4-2. The standard specifies a different format for the back of the PIV card issued to the military, in accordance with the Geneva Convention format as depicted in Figure 4-3. The description of all visual information items follows. Please note that the diagrams below are not to scale.

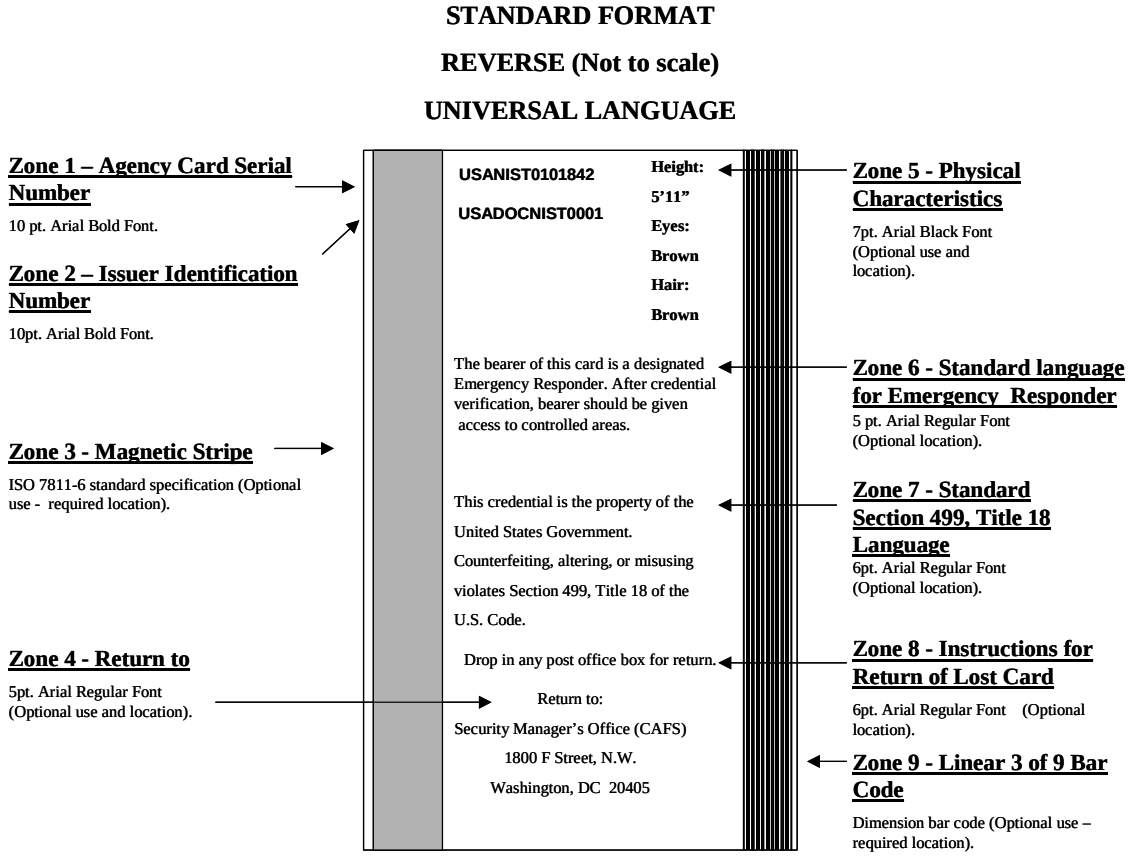
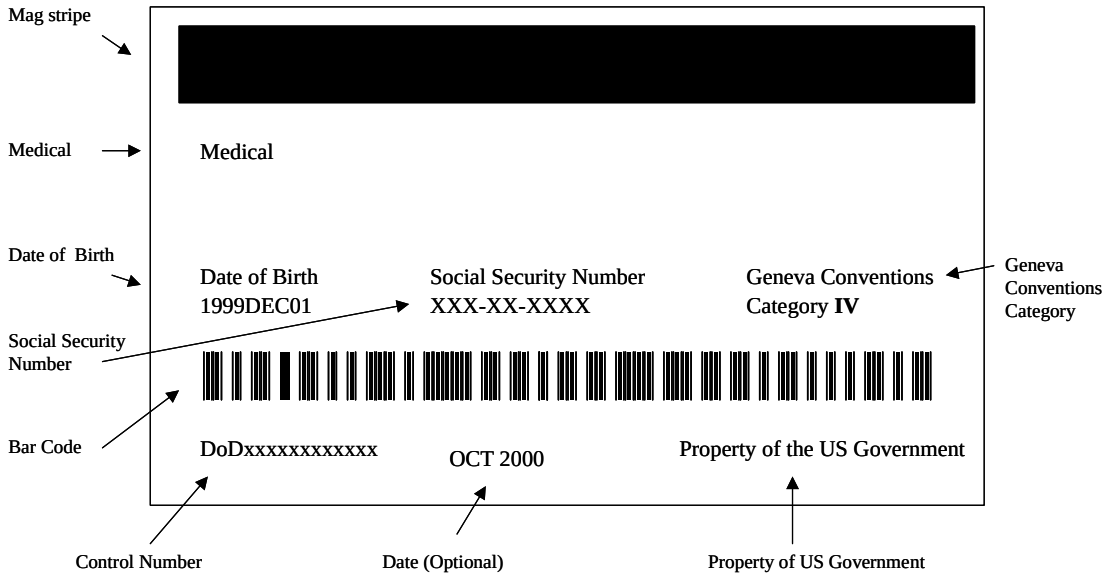


FIGURE 4-2: BACK OF THE CARD

STANDARD FORMAT
REVERSE (Not to scale)
UNIVERSAL LANGUAGE – Military Use



Note: Ghost Image Optional

FIGURE 4-3: BACK OF THE MILITARY PIV CARD

4.1.4.2.a. Zone 1 - Agency Card Serial Number. The first line in Figure 4-2 shall print the issuing Agency's cards unique serial number. The format for this serial number shall be at discretion of the issuing Agency.

4.1.4.2.b. Zone 2 - Issuer Identification. The second line in Figure 4-2 shall print the issuer identifier, consisting of s of six characters for the Department Code, four characters for the Agency Code and a five-digit number that uniquely identifies the issuing facility within the agency.

4.1.4.3 Front of the Card (Optional)
The description of optional information in Figure 4-1 follows.

4.1.4.3.a. Zone 3 - Signature. The agency may print the cardholder signature below the photograph and cardholder name. The space for the signature shall not interfere with the contact and contactless placement requirements.

4.1.4.3.b. Zone 4 - Pay Grade. The pay grade for the cardholder may be printed in this area in a format determined by the issuing Agency.

4.1.4.3.c. Zone 5 - Rank. The rank the cardholder may be printed here in a format determined by the issuing Agency.

4.1.4.3.d. Zone 6 - Bar Code. A bar code may be placed left side of the card surface if applicable to the issuing agency. The agency using [PDF417] bar code shall use this location. This placement shall be as depicted in the diagram (i.e., left side of the card).

4.1.4.3.e. Zone 10 - Agency Name and/or Department. The name of the Agency and/or the cardholder's department may be printed here. The font shall be Arial Black of minimum 7pt size.

4.1.4.3.f. Zone 11 - Agency Seal. The seal for the issuing Agency may be printed on the upper right side of the card. The font shall be Arial Black of minimum 7pt size.

4.1.4.3.g. Zone 12 - Emergency Response Official Identification. The agency may print "Federal Emergency Response Official" above the chip but not in conflict with the contactless placement requirements.

4.1.4.3.h. Zone 13 – Issue Date — The date of card issuance may be printed above the expiration date in the ISO/IEC 8601 format YYYY/MM. The font for the text "Issued" shall be Arial Black of minimum 6pt size. The font for date shall be Arial Black of minimum 10pt size.

4.1.4.4 Back of the Card (Optional)
The description of optional information in Figure 4-2 follows.

4.1.4.4.a. Zone 3 - Magnetic Stripe. The card may contain a magnetic stripe. The magnetic stripe shall be high coercivity and placement will be in accordance with ISO/IEC 7811.

4.1.4.4.b. Zone 4 – Return To. The card may contain a language indicating where the card should be returned if found.

4.1.4.4.c. Zone 5 - Physical Characteristics. The cardholder's physical characteristics such as height, eye color, and hair color may be printed on the back of the card in Arial Black font of minimum 7pt size.

4.1.4.4.d. Zone 6 - Standard Language for Emergency Responder. The standard language for emergency responder may be printed on the back of the card in Arial Regular font of minimum 5pt size. The printed statement shall read "The bearer of this card is a designated Emergency Responder. After credential verification, bearer should be given access to controlled areas."

4.1.4.4.e. Zone 7 - Standard Section 499, Title 18 Language. The standard Section 499, Title 18 language warning against counterfeiting, altering, or misusing the card may be printed below the issuer identification in Arial Regular font of minimum 6pt size.

4.1.4.4.f. Zone 8 - Instructions for Return of Lost Card. Instructions for returning lost cards may be printed on bottom back of the card. The font used for instruction information shall be Arial Regular front of minimum 6pt size. The front used for return address information shall be Arial Regular of minimum 5pt size.

4.1.4.4.g. Zone 9 - Linear 3 of 9 Bar Code. The left corner (from top to bottom) may be used to print bar code. The bar code type shall be of a 3 of 9 barcode in accordance with Association for Automatic Identification and Mobility (AIM) standards.

4.1.5 Logical Credentials

4.1.5.1 Logical Credential Data Model

In order to support a variety of authentication mechanisms, the PIV Logical Credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity via the authentication mechanisms specified at each assurance level. These mandatory data elements collectively comprise the data model for PIV Logical Credentials, and include the following:

- A Personal Identification Number (PIN);
- A Cardholder Unique Identification object (CHUID);
- One asymmetric key pair and corresponding certificate associated with the cardholder;
- Two biometric fingerprints; and
- Biometric facial image.

PIV logical credentials fall into three categories: credential elements used to prove the identity of the cardholder to the card (CTC authentication), credential elements used to prove the identity of the card management system to the card (CMTC authentication), and credential elements used by the card to prove the identity of the cardholder to an external entity (CTE authentication) such as a host computer system. PINs fall into the first category, card management keys in the second category, and the CHUID, biometric information, symmetric keys, and asymmetric keys fall into the third. Biometric information may optionally be used in CTC authentication if the PIV card implements on-card matching of biometric information.

The PIV data model may be extended to meet agency-specific requirements. This specification establishes requirements for 4 classes of optional logical credentials.

- An asymmetric key pair and corresponding certificate for digital signatures;
- An asymmetric key pair and corresponding certificate for key management;
- Asymmetric or symmetric keys for supporting additional physical access applications; and
- Symmetric key(s) associated with the card management system.

4.1.5.2 File Structure

The PIV card architecture described in [SP800-73] defines a Cryptographic Information Application (CIA) in Section 7.1 that contains information about cryptographic keys and other authentication objects that comprise the PIV cardholder's Logical Credentials. A host system can obtain all the information it needs to locate and retrieve biometric information from the card, or to select specific cryptographic keys stored on the card for subsequent cryptographic computations used in challenge-response operations. The host system can therefore dynamically discover the location and file identifiers associated with the Logical Credentials data elements, without the need for a priori knowledge of these. However, the CHUID and biometric

information shall be stored as transparent files in the root file system of the Card Manager (the Master File) to facilitate rapid retrieval for physical access control applications.

It is important to note that the CIA may contain information about other authentication objects associated with applications on the PIV card that are not specified in this standard. This standard only addresses authentication objects that are part of the PIV Logical Credentials.

4.1.6 PIV Card Activation

The PIV card must be activated to perform privileged operations. The PIV card shall be activated for privileged operations only after authenticating the cardholder or the appropriate card management system. Cardholder authentication is described in Section 4.1.6.1 and Card Management system authentication is described in Section 4.1.6.2.

4.1.6.1 Activation by Cardholder

Every PIV card shall implement PIN-based cardholder activation. PIV cards may optionally implement activation using biometric information stored on the card.

For PIN-based cardholder activation, the cardholder shall supply a numeric PIN. The PIN shall be transmitted to the PIV card and checked by the card. If the presented PIN is correct, the PIV card is activated. The PIV card shall include mechanisms to limit the number of guesses an adversary can attempt if a card is lost or stolen. The PIN authentication used by cardholders to activate the PIV card shall meet the identity-based authentication requirements of FIPS PUB 140-2 (i.e., Level 3 Operator Authentication).

For biometric-based cardholder activation, the cardholder shall present biometric information (e.g., a fingerprint) to a reader. The biometric information shall be transmitted to the PIV card, and using biometric match-on-card, compared with the stored biometric information (e.g., image or template). If the presented biometric matches the stored biometric, the PIV card is activated. This specification does not prescribe the type of biometric used for card activation, nor the algorithms or techniques for performing the biometric comparison.

The biometric data used for card activation is a local decision within each department or agency. Where inter-agency interoperability is a concern, agencies that use biometric-based cardholder activation in house should also provide a PIN pad for card activation.

4.1.6.2 Activation by Card Management System

PIV cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card as specified in [GP]. When cards are personalized, card management keys shall be set to be specific to each PIV card. That is, a card issuer may not use a single cryptographic key to activate more than one card.

If supported, card management keys shall meet the algorithm and key size requirements stated in Table 4-1.

Table 4-1: Card Management Algorithm and Key Size Requirements

Card Expiration Date	Algorithm
Through 12/31/2010	Two Key Triple-DES (TDEA2) Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256
After 12/31/2010	Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256

4.2 Cardholder Unique Identifier (CHUID)

The PACS Implementation Guidance [PACS] defines the Cardholder Unique Identifier (CHUID). The CHUID includes a data element, the Federal Agency Smart Credential Number (FASC-N), which uniquely identifies each card. The PIV card shall include an elementary file container continuing the CHUID, as defined in [PACS]. The PIV CHUID includes two additional data elements specific to this standard, and is digitally signed by the issuing authority. CHUID data elements specific to this standard are described below in Section 4.2.1. The format of the CHUID signature element is described in Section 4.2.2 below.

The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV card without card activation. The PIV FASC-N may not be modified post-issuance.

4.2.1 PIV CHUID Data Elements

In addition to the mandatory FASC-N that will uniquely identify a PIV card, the CHUID shall include an expiration date and a position sensitivity level. The expiration date data element will, in machine readable format, specify when the card expires to facilitate status checking and the asymmetric signature field. The expiration date and position sensitivity level were not included in [PACS]; this specification uses tags that were reserved for future use for this data (see Table 4-2) and defines encoding rules for these data elements (see Table 4-3).

Table 4-2: CHUID Additional Expiration Date Data Element

(Cardholder Unique Identifier) CHUID File / Buffer EF 3000 Always Read			
Data Element	**Tag[2]**	**Type**	**Max. Bytes**
Expiration Date	35	Fixed	8
Position Sensitivity	36	Fixed	1
RFU	37-3C		

Table 4-3: CHUID Additional Data Element Definitions.

Data Element	Length (bytes)	Description
Expiration Date	8	Mandatory TLV record. Expiration date in format: yyyymm
Position Sensitivity	1	Mandatory TLV record. Position Sensitivity Level {1,2,3,4} encoded as {0x01, 0x02, 0x03, 0x04} respectively

[2] *The tag values will be accordance with the PACS and the IAB Data Model Task Force Report.*

In addition, [PACS] does not specify a format for the asymmetric signature field. For PIV cards, the format of the asymmetric signature field is specified in Section 4.2.2.

4.2.2 Asymmetric Signature Field in CHUID

This specification requires inclusion of the Asymmetric Signature field in the CHUID container. [PACS] specified a tag for the Asymmetric Signature data element, but does not specify the format. The Asymmetric Signature data element of the PIV CHUID shall be formatted as a Cryptographic Message Syntax (CMS) external digital signature, as defined in [CMS]. The digital signature shall be computed over the entire contents of the CHUID, excluding the Asymmetric Signature field itself. The signature shall be generated by the Issuing Authority using the Issuing Authority's PKI private key. Algorithm and key size requirements for the asymmetric signature are detailed in Table 4-4.

Table 4-4: Algorithm and Key Size Requirements

Card Expiration	Public Key Algorithms & Key Sizes	Hash Algorithms
Through 12/31/2007	RSA 1024 bits or higher; ECDSA 160 bits or higher	SHA-1 hash algorithm
Through 12/31/2010	RSA 1024 bits or higher; ECDSA 160 bits or higher	SHA-1, SHA-224 or SHA-256 hash algorithm
After 12/31/2010	RSA 2048 bits or higher; ECDSA 224 bits or higher	SHA-224 or SHA-256 hash algorithm

The CMS external digital signature must contain the following elements:

- Content shall be encoded in *SignedData*;
- Certificates and Certificate Revocation List (CRLs) shall not be included in the message;
- *SignerInfo*s shall be present and include only a single *SignerInfo*;
- The *SignerInfo* shall:
    - Use the issuerAndSerialNumber choice for SignerIdentifier
    - Specify the Digest Algorithm;
    - Include the digital signature.

The public key required to verify the digital signature shall be available as an X.509 certificate. The certificate shall be a digital signature certificate issued under [COMMON], and shall meet the format and infrastructure requirements for PIV digital signature keys specified in Section 4.3.

4.3 Cryptographic Specifications

At a minimum, the PIV card must store one asymmetric private key, a corresponding public key certificate, and perform cryptographic operations using the asymmetric private key. Cryptographic operations with this key are only performed through the contact interface.

Asymmetric private keys shall be 1024 or 2048-bit RSA keys, or elliptic curve keys of corresponding strength (160 or 224-bit respectively). The PIV card shall implement the following cryptographic operations and support functions:

- RSA or elliptic curve key pair generation
- RSA or elliptic curve private key cryptographic operations
- Importation and storage of X.509 certificates.

The PIV card may include additional asymmetric keys and PKI certificates. This specification defines requirements for digital signature and key management keys. Where digital signature keys are supported, the PIV card is not required to implement a secure hash algorithm (e.g., SHA-1). Message hashing may be performed off-card. As above, useful optional functions include key pair generation and trust anchor storage.

No cryptographic operations are mandated for the contactless interface, but agencies may choose to supplement the basic functionality with storage for a local authentication key and support for a corresponding set of cryptographic operations. That is, if an agency wishes to utilize an AES-based challenge response for physical access, the PIV card must contain storage for the AES key and support AES operations through the contactless interface. If the contactless interface utilizes asymmetric cryptography (e.g., elliptic curve cryptography), the PIV card may also require storage for a corresponding public key certificate.

All cryptographic operations using the PIV keys shall be performed on-card; the PIV card need not implement any additional cryptographic functionality (e.g., hashing, signature verification, etc.) on-card. When used to protect access to sensitive data and systems, this functionality may be augmented (e.g., with hash algorithms and signature verification) by a validated software cryptographic module.

The PIV card has a single mandatory key and four types of optional keys:

- The *PIV authentication* key is an asymmetric private key supporting logical and physical access and is mandatory for each PIV card;
- The *local authentication* key may be either a symmetric (secret) key or an asymmetric private key for physical access and is optional;
- The *digital signature key* is an asymmetric private key supporting document signing and is optional;
- The *key management key* is an asymmetric private key supporting key establishment and transport and is optional; and

- The *card management key* is a symmetric key used for personalization and post-issuance activities.

All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above. All PIV cryptographic keys shall be stored within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above. In addition to an overall validation of Level 2, the PIV card shall provide Level 3 physical security to protect the PIV private keys in storage.

Algorithms and key sizes for each PIV key type are specified in the following table.

Table 4-5: PIV Key Type

PIV Key Type	Time Period	Algorithms & Key Sizes
PIV authentication key	Through 12/31/2010	RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2010	RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher
Local authentication key	Through 12/31/2010	Two Key Triple-DES (TDEA2) Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256 RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2010	Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256 RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher
Digital signature key	Through 12/31/2008	RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2008	RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher
Key management key	Through 12/31/2008	RSA/D-H 1024 bits or higher; ECDH 160 bits or higher
	After 12/31/2008	RSA/D-H 2048 bits or higher; ECDH 224 bits or higher
Card management key	Through 12/31/2010	Two Key Triple-DES (TDEA2) Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256
	After 12/31/2010	Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256

Requirements specific to each storage and access of each class of keys are detailed below. Where applicable, key management requirements are also specified.

- The PIV Authentication Key — The PIV Authentication key shall be generated on the PIV card. The PIV card shall not permit exportation of the PIV authentication key. The PIV authentication key must be available only through the contact interface of the PIV

card. Private key operations may be performed using an activated PIV card without explicit user action (i.e., the PIN need not be supplied for each operation.)

The PIV card shall store a corresponding X.509 certificate to support validation of the public key. The X.509 certificate shall include the FASC-N in the subject alternative name extension to support physical access procedures. The expiration date of the certificate must be no later than the expiration date of the PIV card. Section 5.2.3 of this document specifies the certificate format and the key management infrastructure for PIV authentication keys.

- Local Authentication Key — The PIV card shall not permit exportation of the local authentication key. The local authentication key is used solely for physical access (e.g., to support PACS High assurance authentication). Private/secret key operations may be performed using this key without explicit user action (i.e., the PIN need not be supplied.)

  Cross-agency interoperability is not a goal for the local authentication key. Consequently, this document does not specify key management protocols or infrastructure requirements.

- The Digital Signature Key — The PIV Digital Signature key shall be generated on the PIV card. The PIV card shall not permit exportation of the digital signature key. If present, the digital signature key must only be accessible using the contact interface of the PIV card. Private key operations may be performed using an activated PIV card with explicit user action (i.e., the PIN must be supplied for each private key operation.)

  The PIV card shall store a corresponding X.509 certificate to support validation of the digital signature key. Section 5.2.3 of this document specifies the certificate format and the key management infrastructure for PIV digital signature keys.

- The Key Management Key — The PIV Key Management key may be generated on the PIV card or imported to the card. If present, the key management key must only be accessible using the contact interface of the PIV card. Private key operations may be performed using an activated PIV card without explicit user action (i.e., the PIN need not be supplied for each operation.)

  The PIV card shall import and store a corresponding X.509 certificate to support validation of the key management key. Section 5.2.3 of this document specifies the certificate format and the key management infrastructure for PIV key management keys.

- The Card Management Key — The Card Management key is imported onto the card by the issuer. If present, the card management key must only be accessible using the contact interface of the PIV card. See Section xx (“Activation by Card Management System “) for further details.

The PIV card may also import and store X.509 certificates for use in PKI path validation. These trust anchor certificates may be accessed through the contact interface using an activated PIV card without explicit cardholder action. If supported, initialization and update of trust anchor certificates shall require explicit cardholder action, in addition to activation of the card.

4.4 Biometric Specifications

The biometric data shall be collected and used as follows:

- Ten fingerprints to support law enforcement check during application process,
- Two electronic fingerprints to be stored on the card for automated verification process, and
- An electronic facial image to be stored on the card for alternate identity verification process.

Recognition accuracy rates for fingerprint and facial images have been established by NIST in large-scale trials. Fingerprints shall be primary biometric utilized in the PIV system, as they provide significantly higher accuracy. The recognition rates for facial image is much lower than those of fingerprint images, as it is sensitive to external conditions like illumination and pose.

Index fingerprints are preferred for verification purposes. In case of difficulty in getting index finger prints, an alternate set of finger-pairs could be used in the following decreasing order of preference:

- Thumb
- Middle finger
- Ring finger
- Little finger

The two fingers should not be from the same hand if practicable.

To improve robustness of the fingerprint recognition systems and data interoperability, the format for the storage and exchange of the biometric information captured and used in the PIV system shall conform to established standards. For PIV, one-to-many fingerprint matching shall be performed during the Application process. One-to-one fingerprint matching shall be performed for PIV identity verification.

The biometric data on the PIV card may only be read from an activated card through the contact interface.

4.4.1 PIV Registration (Biometric Enrollment) and Issuance

For the detection of duplicate credentialing and background screening, the PIV registration (biometric enrollment) process requires a one-to-many *biometric identification* search. The biometric data supplied for biometric identification search shall consist of a complete set of ten "slap" fingerprints which may alternatively be accompanied by a set of ten rolled fingerprint images. Although the specific tasks involved in identity-proofing are incremental with respect to the sensitivity-level of the employee or contractor position, law enforcement checks supported by biometric identification are common to all sensitivity levels.

During card personalization, the biometric data from two fingers and a facial image shall be embedded in the PIV card for comparison purposes in subsequent authentication/verification attempts. All biometric data shall be digitally signed by the Issuing Authority. Fingerprint quality and format shall be as described in Section 4.4.2. Facial image quality and format shall be as described in Section 4.4.5. It is also recommended that biometric verification (one-to-one matching) be performed between the enrolled image and a live sample prior to issuance of the card. This improves the confidence in the integrity of authentication during actual card usage.

4.4.2 Fingerprint Representation

Currently, the only representations of fingerprint data that has been proven to provide interoperability between systems are fingerprint *images*. Fingerprint images can accommodate interoperability issues stemming from dissimilar acquisition devices, varying image sizes, resolutions, and grayscale depths (i.e., bits per pixel). Most significantly however, it provides *modular choice of the matching algorithm*.

There are different biometric fingerprint data interchange format standards available for use. Specifically, the ANSI/NIST-ITL 1-2000 (for enrollment), and the ANSI INCITS 381-2004 (for authentication) standards address the interchange of fingerprint images. In addition, ANSI INCITS 378-2004 defines a fingerprint minutiae template that has been developed as a more efficient alternative to image-based exchange. The interoperability of minutiae template data will be tested by NIST in the MINEX04 evaluation scheduled to conclude in late 2005 (http://fingerprint.nist.gov/minex04/).

Exchange of minutiae data has been standardized by ANSI-INCITS 378-2004. This standard is substantially the same as the ISO/IEC 19794-2 currently nearing final international standard status. Although conformance testing standards are currently under development in INCITS M1.3, no conformance standard for minutiae is currently available.

Pending the completion and conclusions of the MINEX04, the interchange of fingerprint image data currently provides the greatest level of interoperability between dissimilar fingerprint recognition systems. It provides implementers of these systems the flexibility to accommodate images captured from dissimilar devices and varying image sizes.

Where electronically submitted, fingerprint images compliant with ANSI/NIST-ITL 1-2000 shall be used for biometric enrollment as described in Section 4.4.3. Fingerprint images compliant with INCITS 381-2004 shall be stored on PIV cards for identity verification as described in Section 4.4.4.

4.4.3 Fingerprint Requirements for Biometric Enrollment

The overall format for recording, storing, and transmitting the biometric information for PIV enrollment shall be as specified in the ANSI/NIST-ITL 1-2000 standard and the CJIS-RS-0010, Electronic Fingerprint Transmission Specification and appendices (EFTS). The captured images shall be plain impressions (also called a *slap* or *flat*) obtained from multiple fingers simultaneously placed on a platen *without* any rolling movement. Alternatively, a corresponding set of rolled images may accompany the plain impressions.

Sets of the required ten fingerprints (not required to be stored on the card) shall be captured through three multi-finger images:

a) Combined impression of the four fingers on the left hand (except for the thumb),

b) Combined impression of the four fingers on the right hand (except for the thumb), and

c) Combined impression of both the left and right thumbs.

The location for each of the fingers within the overall multi-fingerprint images shall be specified within the formatted data as the left, right, top, and bottom pixel locations.

The maximum size for the (a) and (b) images above shall be no greater than 83.3mm X 76.2mm. For the two thumbs, the maximum area shall be no greater than 50.8mm X 76.2mm.

These images shall be referenced through codes 13, 14, and 15, to represent the left four fingers, right four finger, and two thumbs respectively. Table 4-6 lists all of the required fields for the Type 14 ANSI/NIST formatted record used to transmit the enrollment images to the FBI for searching. Additional details addressing the formatting of the data in the ANSI/NIST transaction are contained in Annex C.

Scanning resolution used for image capture should be such that the output of the (delivered) image has a resolution of 500 pixels per inch (ppi), plus or minus 5 ppi, where each pixel represented by eight bits, or 256 grayscale levels. Images shall be captured by devices that have been FBI certified as compliant with the Appendix F requirements of the FBI's Electronic Fingerprint Transmission Specification (EFTS/F).

A certified version of Wavelet Scalar Quantization (WSQ) for 8-bit 500 ppi grayscale images is the acceptable image compression algorithm. Alternate compression algorithms like JPEG 2000 are not recommended since its standard specifies several versions/options and also there is no certified baseline JPEG 2000 version.

The NIST Fingerprint Image Quality (NFIQ) method, discussed in NISTIR 7151 shall be used as the mechanism for making an acquisition-time quality assessment that is predictive of that image's match performance. The NIST NFIQ level must be supplied through a Finger Image Quality field in the Type-14 record. Although the unsegmented fingers shall be contained in the slap images, a unique NFIQ level must be derived and recorded for each finger of the images. This is a mandatory requirement for all slap (flat) fingerprint submissions to the FBI database starting March 2005.

Table 4-6: Field List for Flat Type-14 Record

Identifier	Condition	Field Number	Field Name	Character Type	Field Size Per Occurrence		Occurrences		Maximum Number of Bytes …	Example Data
					Min	Max	Min	Max		
LEN	M	14.001	LOGICAL REC LENGTH	N	4	8	1	1	15	14.001:40164<GS>
IDC	M	14.002	IMAGE DESIGNATION CHAR	N	2	5	1	1	12	14.002:01<GS>
IMP	M	14.003	IMPRESSION TYPE	A	2	2	1	1	9	14.003:0<GS>
SRC	M	14.004	SOURCE AGENCY/ ORI	AN	10	21	1	1	28	14.004:CA0000001<GS>
TCD	M	15.005	TENPRINT CAPTURE DATE	N	9	9	1	1	16	14.005:20040227<GS>
HLL	M	14.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12	14.006:1600<GS>
VLL	M	14.007	VERTICAL LINE LENGTH	N	4	5	1	1	12	14.007:1450<GS>
SLC	M	14.008	SCALE UNITS	N	2	2	1	1	9	14.008:1<GS>
HPS	M	14.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12	14.009:500<GS>
VPS	M	14.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12	14.010:500<GS>
CGA	M	14.011	COMPRESSION ALGORITHM	A	5	7	1	1	14	14.011:1<GS>
BPX	M	14.012	BITS PER PIXEL	N	2	3	1	1	10	14.012:8<GS>
FGP	M	14.013	FINGER POSITION CODE	N	2	2	1	6	25	14.013:13<GS>

Identifier	Condition	Field Number	Field Name	Character Type	Field Size Per Occurrence		Occurrences		Maximum Number of Bytes …	Example Data
					Min	Max	Min	Max		
SEG	M M M M M M	14.021	SEGMENT POSITION FINGER NUMBER LEFT RIGHT TOP BOTTOM	 N N N N N	 1 1 1 1 1	 2 4 4 4 4	2 1 1 1 1 1	4 1 1 1 1 1	99	14.021:10<US>3<US>352<US>725<US>1265<RS> 9<US>375<US>750<US>175<US>765<RS> 8<US>800<US>1150<US>5<US>581<RS> 7<US>1200<US>1598<US>274<US>801<GS>
IQM	M M M	14.022	IMAGE QUALITY METRIC FINGER NUMBER QUALITY SCORE	 N N	 1 1	 2 2	2 1 1	4 1 1	58	14.022:10<US>6<RS>9<US>4<RS>8<US>3<RS>7<US>3<GS>
DAT	M	14.999	IMAGE DATA	B	2	--	1	1	--	14.999:<IMAGE DATA OMPRESSED@15:1> <FS>

4.4.4 Fingerprint Requirements for Identity Verification

This standard requires the capture of the fingerprint image from the left and right index fingers for the purpose of PIV card authentication. The PIV card format requirements for the capture, recording, storing, and transmitting the biometric information for PIV authentication shall be as specified in the ANSI/INCITS 381-2004 standard. Likewise, the compression algorithm, image resolution, and pixel depth requirements for authentication shall be the same as specified for card enrollment. At the authentication station, two fingerprints shall be captured: (a) an impression of the left index finger and (b) and an impression of the right index finger. These images shall be processed and compared to the images on the card and a subsequent threshold-based decision apparatus will render a verification decision.

ANSI/INCITS 381-2004 stipulates that individual finger records be embedded within a Common Biometric Exchange File Format (CBEFF) [NISTIR 6529-2001]. The fingerprint records generated for PIV card approval will be embedded in such a CBEFF-compliant data structure. The identification that the finger records conform to ANSI/INCITS 381-2004 should be provided in the appropriate locations in the CBEFF embedding record through the Format Owner and Format Type Code fields with values 0x001B (decimal 27) and 0x0401 (decimal 1025) respectively.

4.4.5 Face Representation

This standard supports the use of facial images in three circumstances:

- **Unavailable Fingerprints —** When Applicants are unable to present fingerprints, because of disability for example, the facial image may be used.

- **Multimodal Applications —** The facial image may be used in conjunction with the fingerprint image if lower false acceptance rates are required.

- **Visual Inspection —** The electronic facial image may be used by a human inspector in a formalized process for identity verification.

Facial images must comply with all normative clauses of ANSI/INCITS 385-2004. Because that standard is generic across many applications it includes clauses that have either-or requirements. The following paragraphs give specific PIV requirements for such cases.

4.4.5.1 Image Type

The face record format used for PIV shall comply with all requirements of the Token Image Type defined in the Section 9 of ANSI/INCITS 385-2004. The Token specification defines geometrical properties of the face relative to the image. Particularly the center's of the subject's eyes must be located and placed at specific pixel locations. Thus PIV implementations shall locate the eyes, either automatically or manually, and rotate and translate the image to conform to the Token geometry.

4.4.5.2 Expression

The PIV card facial image shall be acquired from an applicant with a neutral facial expression.

4.4.5.3 Image Color Space

The image data shall be encoded in the YUV color space with 422 chrominance subsampling.

4.4.5.4 Resolution

Face recognition performance is a function of the spatial resolution of the image [NISTIR 7083]. Face resolution is conventionally specified by the distance, in pixels, between the centers of the subject's two eyes. The PIV card image shall have an eye-to-eye resolution of 120 pixels – the higher resolution shall be used if the PIV card has sufficient storage capacity. Images shall be acquired such that their native resolution is greater than or equal to 120 pixels from eye-to-eye. Acquisition at lower resolutions with subsequent interpolation shall not be applied. Scaling of images from larger sizes to achieve the 120 pixel specification shall be done in one step.

4.4.5.5 Compression

Because PIV cards are likely to have limited storage space, and face recognition performance has been demonstrated to be sensitive to compression ratio [NISTIR 7083], we need to have a trade off in choosing the correct compression ratio. PIV images shall be compressed using the baseline JPEG compression algorithm using a 30: 1 compression ratio. This provides images with required accuracy without consuming too much of storage space.

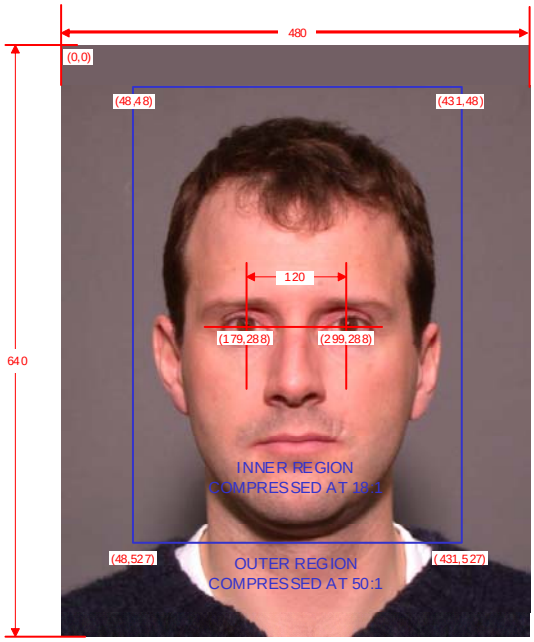


FIGURE 4-4: GEOMETRY OF THE TOKEN 120 FACIAL IMAGE

The images shall be acquired in a raw form and shall not at any intermediate stage be compressed in any way other than that mandated for the final Token image. The image can be acquired from a person in a digital form using a digital camera that can generate image meeting the pixel requirements. Image acquisition systems should not apply compression before the eye-location, scaling, rotation and translation operations are performed during preparation of the Token image.

Table 4-7: Facial Image Property

Property of Token 120 Image	Value
Eye-to-eye (pixels)	120
Image width (pixels)	480
Image height (pixels)	640
Inner region width (pixels)	384
Inner region height (pixels)	480
Uncompressed data size (bytes) color space: YUV 422	460800
Compression ratio for baseline JPEG compression	30:1

4.4.5.6 Distortion

All image acquisition system shall follow the guidelines in Section A8 of ANSI/INCITS 385 to produce a standard radial distortion.

4.4.5.7 Background

The PIV card image shall be acquired with the subject in front of a uniform background.

4.4.5.8 Quality

As part of the PIV enrollment process, an automated assessment of facial image quality shall be made while the human subject is present. A quality measuring implementation, for which a certification and calibration may be required, should produce a value on the range 1 to 100 which shall be used given the following interpretations be interpreted as follows:

Table 4-8: Facial Image Quality

Quality Value	Meaning	Action
81-100	No defects are present	Accept and enroll
61-80	Minor defects are present	Accept and enroll
41-60	Some tolerable defects are present	Reacquire unless timeout has been reached. If timeout reached accept best image.
21-40	Unacceptable for enrollment when reacquisition is possible	Reacquire unless timeout has been reached. If presentation limit has been reached inspect equipment and environment. Require subject to return.
1-20	Unacceptable for enrollment and one-to-many operations	Reacquire. If presentation limit has been reached inspect equipment and environment, then seek vendor support if no apparent cause of failure. Require subject to return later.

Low quality values shall be reported if the face is non-frontal or rotated, is not located centrally or is cropped, if the image is blurred, over or under exposed, or is compressed in a manner inferior to that specified in this standard. In any case, quality values shall be developed and assigned such that they are ultimately indicative of true and/or false accept rates in verification or identification.

A standard for conformance of facial images to ANSI/INCITS 385 is under development.

4.4.6 Protection of Biometrics

The mechanisms provided by the PIV card must protect biometric data in storage. Signatures on biometrics stored on the PIV card shall be formatted as a CMS external signature, as defined in [RFC 3852]. The digital signature shall be computed over concatenation of the following CBEFF elements:

- CBEFF Header Version (If Present);
- Patron Header Version;

- Biometric Type (If Present);
- Record Data Type (If Present);
- Record Purpose (If Present);
- Record Data Quality (If Present);
- Creation Date (If Present);
- Creator (If Present);
- Biometric Specific Memory Block (BSMB) Format Owner;
- BSMB Format Type; and
- BSMB.

The CMS external digital signature must contain the following elements:

- Content shall be *SignedData*;
- Certificates and CRLs shall not be included in the message;
- *SignerInfo*s shall be present and include only a single *SignerInfo*
- The *SignerInfo* shall:
    - Use the *issuerAndSerialNumber* choice for *SignerIdentifier*
    - The authenticated attributes shall be present and include a *serialnumber* attribute with the FASC-N for the PIV card
    - Include the digital signature.

Additional information, such as the cardholder's name or the distinguished name in the cardholder's PKI certificates may be included in the SignerInfo authenticated attributes.

4.5 Card Reader Specifications

4.5.1 Contact Reader Specifications

Contact card readers shall conform to ISO/IEC 7816 Standards for the card-to-reader interface. These readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface.

4.5.2 Contactless Reader Specifications

Contactless card readers shall conform to ISO/IEC 14443 [ISO 14443] standard for the card-to-reader interface. In cases where these readers are connected to general purpose desktop computing systems, they shall conform to [PCSC] for the reader-to-host system interface. In physical access control systems where the readers are not connected to general purpose desktop computing systems, the reader-to-host system interface is not specified in this standard. This is necessary in order to allow retrofitting of PIV readers into existing physical access control systems that use a variety of nonstandard card reader communications interfaces.

4.5.3 PIN Pad Specifications

PIV cards may be activated through the contact interface by the cardholder using the mandatory PIN described in Section 4.1.5. Where the PIV card is used for physical access, the PIN pad shall be incorporated into the reader. Where the PIV card is used for logical access (e.g., to authenticate to a website or other server), the PIN pad may be incorporated into the reader or the PIN may be entered using the computer's keyboard.

5 PIV ISSUANCE AND MANAGEMENT

5.1 Card Issuance and Management Subsystem

5.1.1 Registration Database

The Registration Database is representative of the storage location(s) that hold PIV registration and cardholder data. This standard does not specify the type schema, or interfaces for the registration repository. The standard does require that access to the registration repository shall be closely controlled with only authorized individuals allowed to read and/or modify contained information.

5.1.2 PKI Repository and OCSP Responder(s)

The PIV PKI Repository and On-line Certificate Status Protocol (OCSP) Responder are intended to provide PIV card and key status information across agencies and organizations, to support high assurance interagency PIV card interoperation. Agencies will be responsible for notifying Certificate Authority (CA) when cards or certificates are revoked. CAs shall maintain the status servers and responders needed for PIV card and certificate status checking.

The expiration date of the authentication certificate shall not be after the expiration date of the PIV card. If the card is revoked, the authentication certificate shall be revoked. However, an authentication certificate (and it's associated key pair) may be revoked without revoking the PIV card, and may then be replaced. A current, unexpired PIV authentication certificate on a card is proof that the card was issued and is not revoked.

Since the lifetime of authentication certificates is long, typically several years, a certificate revocation mechanism is necessary. Two are conventional: the CRL and the OCSP. CAs that issue PIV authentication certificates shall maintain a Lightweight Directory Access Protocol (LDAP) directory server that holds the CRLs for the certificates it issues, as well as any CA certificates needed to build a path to the Federal Bridge CA.

Certificates shall contain the crlDistributionPoint or authorityInformationAccessPoint extensions needed to locate CRLS and the authoritative OCSP responder. In addition, every CA that issues PIV authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues.

5.2 Card Issuance and Management Processes

The requirements specified in this Section are in addition to those specified in Section 2.2 (PIV-I).

5.2.1 PIV Application and Approval

5.2.1.1 New Employees

An Applicant applies for an identity credential as a part of the vetting process for Federal employment. An Applicant provides two forms of identification from the list of acceptable documents included in the *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification* to the PIV Registration Authority. At least, one of the documents shall be a valid State or

Federal Government-issued picture ID. The PIV Requesting Official shall submit the PIV request and photocopies of identity source documents for the Applicant to the PIV Authorizing Official. The PIV Authorizing Official shall approve the request and forward it together with photocopies of the identity source documents to the Registration Authority and the PIV Issuing Authority.

The PIV request form shall include:

- Name, organization and contact information of the PIV Requesting Official;
- Name, position including the position sensitivity level, and contact information of the
- Applicant including address of Applicant's parent organization;
- Name, organization and contact information of the PIV Authorizing Official,
- Name and contact information for the issuing organization,
- Signatures of the Requesting Official and the Authorizing Official.

Based on the required position sensitivity level, the Applicant shall complete the appropriate background information form listed Table 5-1.

Table 5-1: Background Information Forms Required from Applicant

Position Sensitivity Level	Form
1	Form I-9, OMB No. 1115-0136, Employment Eligibility Verification
2	Standard Form 85, OPM Questionnaire for Non-sensitive Positions or equivalent
3	Standard Form 85 P, OPM Questionnaire for Public Trust Positions or equivalent
4	Standard Form 85 P, OPM Questionnaire for Public Trust Positions or equivalent

The Applicant shall provide the completed background information form to the Registration Authority. In addition, the Applicant shall appear in person and provide two forms of identity source documents originally provided to the PIV Requesting Official. The Registration Authority shall visually inspect the identity source documents and authenticate them as being acceptable. In addition, the Registration Authority shall compare the picture on the source document to the applicant to ensure the applicant is the holder of the identity source document. At this time, the Registration Authority shall fingerprint the Applicant by collecting all of the Applicant's fingerprints as defined in Section 4.4.3. The Registration Authority shall conduct the appropriate background check as defined in Table 5-2 using the position sensitivity level from the PIV Request Form for the Applicant. Two of the Applicant's fingerprints shall be securely maintained for personalization of the Applicant's PIV card as defined in Section 4.4.4. The Registration Authority may optionally also photograph the Applicant for personalization of the PIV card.

After successful completion of the appropriate background check, the Registration Authority shall securely notify the Issuing Authority that a PIV card can be issued to the Applicant.

The Registration Authority shall be responsible to maintain:

- Completed and signed PIV Request Form,
- Copies of the identity source documents,
- Completed and signed background form received from the Applicant,
- Results of the required background check,
- Any other materials used to prove the identity of the Applicant.

Table 5-2: Background Checks By Position Sensitivity Level

Position Sensitivity Level	Personal Identity Background Checks
1 Low	Authentication of Applicant Identity Source Documents conducted by entity responsible for authorizing PIV card issuance (checking and verifying validity with each Document's Issuer). Law enforcement check (fingerprint).
2 Moderate	National Agency Check and Inquiries (NACI)
3 High	NACI and Credit Check (NACIC)
4 Critical (Vital National Asset-Critical Infrastructure)	Limited Background (LBI) or Background Investigation (BI)

5.2.1.2 Current Employees

A similar application and approval process shall be followed for current employees expect that background checks are not required if the results of the most recent previous check are on-file and can be referenced in the application and verified by the Registration Authority.

5.2.1.3 Overseas Foreign Workers

For citizens of foreign countries who are working for the U.S. Federal Government overseas, a similar process for application and approval must be established using a method approved by the Office of Management Budget.

5.2.2 PIV card Issuance

The Issuing Authority shall confirm the validity of the notification from the Registration Authority. The Issuing Authority shall digitally sign biometrics (facial image and the two

fingerprints), received from the Registration Authority, and store them on the PIV card during personalization. The Applicant may be asked to provide a PIN, or the Issuing Authority may generate a PIN on their behalf.

The Applicant may generate cryptographic key pairs and obtain the corresponding certificates at this time. Alternatively, the Applicant may be supplied a one-time authenticator for use in subsequent certificate requests. In this case, the Applicant will generate their own key pairs at their own workstation.[3] The identity token is initialized for the Applicant and issued. Actual issuance may occur during the initial visit to the Issuing Authority or may occur at a later date.

Simultaneously during the issuing stage, the recipient's name, the issuer identity, the card number, and possibly PKI certificate identification information are enrolled and registered with the backend database that supports the PIV system. Depending on the infrastructure design, this backend may be centralized or decentralized.

5.2.3 Key Management

PIV cards consistent with this specification may have one, two, or three asymmetric private keys. To manage the associated public keys, agencies are required to issue and manage X.509 public key certificates as specified below:

5.2.3.1 Architecture

Certificate Authority (CA) that issue certificates to support PIV card authentication shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI. Self-Signed, Self-issued, and CA certificates issued by these CAs shall conform to *Worksheet 1: Self-Signed Certificate Profile*, *Worksheet 2: Self-Issued CA Certificate Profile*, and *Worksheet 3: Cross Certificate Profile* respectively in [PROF].

5.2.3.2 PKI Certificates

All certificates issued to support PIV card authentication shall be issued under the id-CommonHW policy and the id-CommonAuth policy[4] as defined in the *X.509 Certificate Policy for the Common Policy Framework* [COMMON]. These requirements cover identity proofing as well as the management of certification authorities (CAs) and registration authorities (RAs). CAs and RAs may be operated by agencies, or outsourced to PKI Service Providers. For a list of PKI Service Providers who have been approved to operate under [COMMON], see http://www.cio.gov/ficc/cpl.htm

[COMMON] requires FIPS 140-2 Level 2 validation for the subscriber cryptomodule (i.e., the PIV). In addition, this specification requires the cardholder to authenticate to the PIV card each time it performs a private key computation with the *digital signature key* or *key management key.*

[COMMON] imposes a minimum of RSA key length of 1024 bits for CA key sizes, and mandates use of SHA-1 and SHA-256 hash algorithms. CAs must use 2048 bit RSA keys when signing certificates and CRLs that expire on or after December 31, 2008. CAs that generate certificates and CRLs under this policy shall use SHA-1 or SHA-256 hash algorithm when

---

[3] *Note that the issuing agency is responsible for the necessary PKI certificate management.*

[4] *The id-CommonAuth policy has not yet been drafted. This policy will be used to differentiate simple authentication keys, where user interaction is not required, from signature keys where the operation is expected to demonstrate explicit user intent.*

generating digital signatures. Signatures on certificates and CRLs that are issued before January 1, 2007 shall be generated using SHA-1. Signatures on certificates and CRLs that are issued between January 1, 2007 and December 31, 2009 (inclusive) shall be generated using either SHA-1 or SHA-256. Signatures on certificates and CRLs that are issued on or after January 1, 2009 shall be generated using SHA-256.

Note that additional cryptographic algorithms (e.g., ECDSA) are specified in the following text. Future enhancements to [COMMON] are expected to permit use of additional algorithms. For conformance to this specification, PIV card management systems are limited to algorithms and key sizes recognized by this standard and the current version of [COMMON].

5.2.3.2.1 X.509 Certificate Contents

The required contents of X.509 certificates associated with PIV private keys are based on the X.509 Certificate and CRL Profile for the Common Policy [PROF]. The relationship is described below:

- HTTP URIs required by [PROF] in the SIA, AIA, and CDP extensions are optional for this specification;

- AIA extensions shall include pointers to the appropriate OCSP status responders, using the id-ad-ocsp access method as specified in Section 8 of [PROF], in addition to the LDAP URIs required by [PROF].

- If private key computations can be performed with the *PIV authentication key* without user intervention (beyond that required for cryptomodule activation), the corresponding certificate must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension.

- Certificates containing the public key associated with a digital signature private key shall conform to *Worksheet 5: End Entity Signature Certificate Profile* in [PROF].

- Certificates containing the public key associated with a PIV authentication private key shall conform to *Worksheet 5: End Entity Signature Certificate Profile* in [PROF], but shall not assert the nonRepudiation bit in the keyUsage extension and must include the PIV card's FASC-N in the subject alternative name field.

- Certificates containing the public key associated with a key management private key shall conform to *Worksheet 6: Key Management Certificate Profile* in [PROF].

- Requirements for algorithms and key sizes for each of the three types of PIV asymmetric keys are given in the Table 5-3.[5]

[5] *The current text of [COMMON] permits only RSA with SHA-1 and SHA-256. Supporting DSA, Diffie-Hellman and elliptic curve algorithms will require a change in [COMMON].*

Table 5-3: PIV Private Key Type

PIV Private Key Type	Certificate Expiration Date	Algorithms & Key Sizes
PIV authentication key	Through 12/31/2010	RSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2010	RSA 2048 bits or higher; ECDSA 224 bits or higher
Digital signature key	Through 12/31/2007	RSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2007	RSA 2048 bits or higher; ECDSA 224 bits or higher
Key management key	Through 12/31/2007	RSA/D-H 1024 bits or higher; ECDH 160 bits or higher
	After 12/31/2007	RSA/D-H 2048 bits or higher; ECDH 224 bits or higher

5.2.3.3 X.509 CRL Contents

CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum. The contents of X.509 CRLs shall conform to *Worksheet 4: CRL Profile* in the X.509 Certificate and CRL Profile for the Common Policy [PROF].

5.2.3.4 Certificate and CRL Distribution

This specification requires distribution of CA certificates and CRLs using the LDAP. At a minimum, CA certificates and CRLs shall be distributed using LDAP. Specific requirements are found in *Table II - Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements* of the Shared Service Provider Repository Service Requirements [SSP REP].

Considering that authentication certificates contain the FASC-N in the subject alterative name extension, these shall not be distributed via LDAP. It is an agency decision whether or not other user certificates (digital signature and key management) are distributed via LDAP. When user certificates are distributed, the requirements in *Table IV – End-Entity Certificate Repository Service Requirements* of [SSP REP] shall be satisfied.

5.2.3.5 OCSP Status Responders

OCSP status responders shall be implemented as a supplementary certificate status mechanism. The OCSP status responders must be updated at least as frequently as CRLs are issued. The definitive OCSP responder for each certificate shall be specified in the AIA extension as described in [PROF].

5.2.3.6 Migration from Legacy PKIs

Agencies whose PKI has cross-certified with the Federal Bridge CA (FBCA) at Medium or High may continue to assert agency specific policy OIDs through December 31, 2007. Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Agencies may continue to assert agency specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)

5.2.4 PIV Card Maintenance

Although PIV cards may be issued by issuing authorities as per the specifications laid out in this standard, these cards may not remain valid through their expiration date. The cardholder may retire, change jobs, or be fired, invalidating a previously accurate card. The PIV System must ensure this information is distributed efficiently, both within the PIV management infrastructure and to parties authenticating a cardholder. In this regard, procedures for PIV card maintenance must be integrated into agency procedures to ensure effective card management.

5.2.4.1 Renewal

A cardholder shall apply for a renewal when a valid PIV card expires. The Issuing Authority will verify the cardholder identity against the biometric information stored on the expiring card. In the event of expired, lost, or stolen card, re-issuance procedures in Section 5.2.4.2 shall be followed.

A new facial image shall be collected and stored on the PIV card. The fingerprint from the expired PIV card may be stored on the new PIV card; note that the digital signature must be recomputed with the new FASC-N.

Since the expiration date of the PIV authentication certificate and optional digital signature certificate cannot be after the expiration date of the PIV card, a new PIV authentication key and certificate shall be generated. If the PIV card supports the optional key management key, it may be imported to the new PIV card. The expired PIV card must be collected by the registration authority and destroyed.

The Parent Organization shall verify that the employee remains in good standing and personnel records are current prior to renewing the card and associated credentials.

5.2.4.2 Re-issuance

In case of re-issuance, a new personalization, including fingerprint and facial image capture, shall be conducted. The Parent Organization shall verify that the employee remains in good standing and personnel records are current prior to renewing the card and associated credentials.

A cardholder shall apply for re-issuance when the PIV card is expired, compromised, lost, or stolen. The cardholder can also apply for re-issuance of a valid PIV card in the event of an employee status or attribute change or if one or more logical credentials have been compromised. A re-issuance of the electronic information and cryptographic keys on the card may also be necessary if the contents of the card are locked due to the usage of an invalid PIN. However, PIN resets may be performed by well laid out and documented procedures by each individual agency.

When these events are reported, normal operational procedures must be in place to ensure that:

The PIV card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status.

- The PIV Certificate Issuer shall be informed and the certificate corresponding to PIV authentication key on the PIV card must be revoked. Agencies may revoke certificates corresponding to the optional digital signature and key management keys. CRLs issued shall include the appropriate certificate serial numbers.

- OCSP Responders shall be updated so that queries with respect to certificates on the PIV card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records.)

- For attributes changes, the registration authority must verify the reason for the change and keep a copy for records.

Where possible, the PIV card shall be collected and destroyed. Where the card cannot be collected, normal operational procedures shall complete within 18 hours of notification. In some cases, 18 hours is an unacceptable delay. For example, an agency may discover a cardholder's true identity is a person on a terrorist watch list. In such a case, emergency procedures must be executed to disseminate this information as rapidly as possible. Agencies are required to have procedures in place to update all servers in one hour in the case of such an emergency.

5.2.4.3 PIV Update

For a special case, where a position sensitivity level is increased, the PIV card may be updated rather than replaced. Update processes shall include:

- Update position sensitivity level in the CHUID,

- Recompute the CHUID digital signature, and

- Store the signed CHUID on the PIV card.

The Applicant's identity shall be reverified as in the case of PIV renewal (Section 5.2.4.1). The Issuing Authority shall verify Applicant's new position sensitivity level and completion of identity proofing requirements before updating the PIV card.

5.2.5 PIV Card Termination

The termination process is used to permanently destroy or invalidate the usage of the card including the data on it including the keys such that it cannot be used again. The PIV card shall be terminated under the following circumstances:

- An employee separates (voluntarily or involuntarily) from Federal service;

- An employee separates (voluntarily or involuntarily) from the Federal contractor;

- A contractor changes positions and no longer needs access to Federal buildings or systems;
- A cardholder is determined to hold a fraudulent identity; or
- The cardholder passes away.

Similar to the situation in which the card or a credential is compromised, normal termination procedures must be in place as to ensure that:

- The PIV card is collected and destroyed.
- The PIV card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status.
- The PIV Certificate Issuer shall be informed and the certificate corresponding to PIV authentication key on the PIV card must be revoked. Agencies may revoke certificates corresponding to the optional digital signature and key management keys. CRLs issued shall include the appropriate certificate serial numbers.
- OCSP Responders shall be updated so that queries with respect to certificates on the PIV card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records.)

6 PIV CARD AUTHENTICATION

This informative Section discusses authentication mechanisms that are supported by the PIV card and the credentials it hosts. Within the context of the PIV card, *identity authentication is defined as the process of establishing confidence in the identity of the cardholder presenting a PIV card*. The authenticated identity of the cardholder can then be used by an agency to make an access decision (to controlled Federal Resources) based on the agency's own authorization mechanisms and local access control policy. Thus, this Section should be treated as Informative.

This Section also discusses the use of the PIV card authentication mechanisms for support of physical and logical access control systems. It may be noted that the scope of this standard extends to providing a number of authentication mechanisms in "support" of agency defined access control and authorization policies. Nothing in this standard should be interpreted as prescriptive in terms of the authorization checks and access control policies implemented by a Federal agency.

6.1 PIV Card Authentication Mechanisms

The fundamental purpose of the PIV card is to serve as a means of authenticating the identity of the PIV cardholder for access to Federal resources. Thus, the PIV card supports identity authentication in environments that are equipped with card readers as well as environments that are without card readers. In environments where the access control point is not equipped with suitable PIV card readers, visual authentication is usually performed.

The PIV card may also be used in an access control environment where PIV card readers are available. In this case, electronic authentication of the cardholder may be conducted using the PIV card. Card readers may be contactless or contact-based. Contactless card readers are used to support contactless authentication of the PIV card. For privacy reasons, contactless use of PINs and biometrics is not supportedPINs and biometrics may be used with the PIV card using contact readers.

In the following subsections, various types of authentication mechanisms that may be supported by the PIV card are discussed. It is important to note that these are authentication mechanisms that are available as options to agency resource owners as they implement access control systems for protecting their resources. This standard provides descriptions of these mechanisms to assist in the implementation of authentication mechanisms for controlling access to Federal resources. It should also be noted that agencies can implement compound authentication mechanisms by using the basic authentication mechanisms specified in this Section.

6.1.1 Authentication using PIV Visual Credentials

Visual authentication of a PIV cardholder is essential in environments where electronic verification infrastructures are either not installed, or temporarily unavailable (due to network outages and system malfunction). Visual identity authentication may be used to support access control to physical facilities and resources. However, since a human verifier is needed to implement visual identity verification, this type of verification should not be used to support access control to logical resources.

The PIV card has a number of mandatory topographical features (in the front and back), that support visual identification and authentication, namely:

- Photograph
- Name
- Employee Affiliation Employment Identifier
- Expiration Date
- Agency Card Serial Number (back of Card)
- Issuer Identification (back of Card)

The PIV card may also bear the following optional components:

- Agency Name and/or Department
- Agency Seal
- PIV Card Holder's Physical Characteristics
- Signature

When a PIV cardholder attempts to pass through an access control point for a Federally controlled resource or facility, a human guard can perform visual identification and authentication of the cardholder, and determine whether the identified individual should be allowed through the control point. The series of steps that may be applied in the visual authentication process are as follows:

1) The human guard at the access control entry point determines whether the PIV card appears to be genuine and has not been tampered with in any way.

2) The guard compares the cardholder's facial features with the picture on the card to check that they match.

3) The expiration date on the card is checked to ensure that the card has not expired.

4) The cardholder's physical characteristic descriptions are compared to those of the cardholder. (OPTIONAL)

5) The cardholder's signature is collected and compared with the signature on the card. (OPTIONAL)

6) One or more of the other data elements on the card (e.g. Name, Employee Affiliation Employment Identifier, Agency Card Serial Number, Issuer Identification, and Agency Name) are used to determine whether access should be granted to the cardholder.

6.1.2 Authentication using the PIV CHUID

The PIV card provides a mandatory cardholder Unique Identifier (CHUID) container that is an Elementary File (EF). The CHUID data model comprises a number of data elements as described in Section 4.2.

In environments that support electronic interaction with the PIV card, simplistic authentication mechanisms may be implemented, using the data elements contained within the CHUID. In this type of authentication mechanism, there is no attempt to correlate the data and identifiers on the card with the actual cardholder. It is assumed that the cardholder is the owner of the card, and the identifiers read from the card are passed on to the access control decision module. Since CHUID-based authentication mechanisms are inherently weak, they may be suitable for certain physical access control environments; however, these mechanisms are not recommended for logical access control systems.

The CHUID data elements may be used for authentication sequence as follows:

1) The CHUID is read from the PIV card.

2) The digital signature on the CHUID is checked to ensure CHUID is intact and comes from a trusted source. (OPTIONAL)

3) The Expiration Date is checked to ensure that the card has not expired. (OPTIONAL)

4) One or more of the CHUID data elements (FASC-N, Agency Code, DUNS, Position Sensitivity) are used as input to the authorization check to determine whether the cardholder should be granted access.

A specific variant of the above sequence is described in the Physical Access Control System (PACS) LOW assurance profile. This is described in detail in [PACS]. Another variant of the CHUID-based authentication that may be used comprises the following steps:

1) The CHUID and the Card Unique ID (CUID) are read from the PIV Card.

2) The digital signature on the CHUID is checked to ensure CHUID is intact and comes from a trusted source. (OPTIONAL)

3) The Expiration Date is checked to ensure that the card has not expired. (OPTIONAL)

4) One or more of the CHUID data elements as well as the CUID are passed through a unidirectional cryptographic transform that uses a site-specific key, such as a hashed message authentication code algorithm. The result of the cryptographic transform and CHUID and CUID elements are passed as input to the authorization function.

The above authentication mechanism is aligned with the Physical Access Control System (PACS) Medium assurance profiles, described in detail in [PACS].

6.1.3 Authentication using PIV Biometric Credentials

In environments where the collection of a PIN and a biometric sample from the cardholder is feasible, a strong authentication mechanism that ties the cardholder to the card itself may be implemented. Depending upon the rigor of the checks that are used during the authentication process, this type of mechanism can be applied to logical as well as physical access control systems.

The PIV card hosts a signed biometric that can be read from the card after the cardholder provides a PIN to perform CTC authentication. The signed biometric may be used to support an authentication mechanism through a match-off-card scheme as follows:

1) The cardholder is prompted to submit a PIN, activating the PIV card and allowing the signed biometric to be read from the card.

2) The signed biometric is read from the PIV card.

3) The signature on the biometric is verified to verify that the biometric is intact and comes from a trusted source. (OPTIONAL[6])

4) The cardholder is prompted to submit a live biometric sample.

5) If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.

6) The CHUID is then read from the card.

7) The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.

8) The Expiration Date in the CHUID is checked to ensure that the card has not expired. (OPTIONAL)

9) One or more of the CHUID data elements (FASC-N, Agency Code, DUNS, Position Sensitivity) are used as input to the authorization check to determine whether the cardholder should be granted access.

6.1.4 Authentication Using PIV Symmetric Cryptography

The PIV card may optionally support the PACS compliant symmetric key cryptographic data model and functions. The PACS site-specific symmetric key is stored a PIV local authentication key as defined in Section 4.3. The PIV card supports PACS compliant challenge-response based authentication schemes that use symmetric cryptography, as in the following sequence:

1) The CHUID is read from the card.

---

6 *The signature verification is optional only for access control implementations that do not have access to the Agency network and cannot fully verify the digital signature on the biometric.*

2) The expiration date in the CHUID is checked to ensure that the card has not expired. (OPTIONAL)

3) The reader issues a challenge string to the card requests a symmetric operation in response.

4) The response received from the card is compared with a parallel computation using selected data elements from the CHUID, along with a site-specific symmetric key to check that they match.

5) The CHUID elements are passed as input to the authorization function.

The above authentication mechanism is aligned with the PACS High assurance profiles, as described in detail in [PACS].

6.1.5 Authentication using PIV Asymmetric Cryptography

In access control environments where asymmetric cryptographic capabilities are available, the PIV card may be used to perform identity authentication using asymmetric key mechanisms. The PIV card carries a mandatory asymmetric authentication private key and corresponding certificate, as described in Section 4.3. The PIV card can support an asymmetric authentication mechanism comprising the following steps:

1) The reader issues a challenge string to the card and requests an asymmetric operation in response.

2) The cardholder presents their PIN or biometric sample. The authentication information is submitted to the card, is verified, and the card is activated.

3) The card responds to the challenge by signing it using the authentication private key, and attaching the associated certificate

4) The response signature is verified and standards-compliant PKI path validation is conducted. The related digital certificate is checked to be from a trusted source.

5) The response is validated as the expected response to the issued challenge.

6) The Subject DN or FASC-N from the authentication certificate is extracted and passed as input to the authorization function.

6.2 Authentication for Physical Access Control

The PIV card can be used to authenticate the cardholder in a physical access control environment. For example, a Federal facility may have physical entry doors that have human guards at checkpoints, or have electronic access control points.

PIV cards can be used for physical access control in a visual, contactless or a contact-based environment. Visual authentication may be used alone or to supplement a contactless or contact-based authentication process.

Within a contactless environment, the card is able to get power for a very brief period and can only participate in a very rapid authentication dialogue with the reader. Additionally, contactless cards/readers are usually deployed in high volume usage environments where rapid authorization decisions need to be made. Hence, implementations that require complex computational operations or lengthy backend verification processes are typically less suitable for the contactless environment.

For contact-based physical access control, the card is able to draw power directly from the card reader and can hence participate in more complex protocol interchanges with the reader. Additionally, these mechanisms make use of cardholder PIN or biometric.

6.2.1 Assumptions and Constraints

The physical access environment typically has the following characteristics:

- The environment may need to support a medium to high volume of entry, which implies that the time required for authenticating a single cardholder has to be very short.

- Physical access control points are typically not connected to an agency's logical network or the Internet. Hence mechanisms that rely upon online key management techniques or status lookups are not practical.

Thus, typical electronic physical access control systems are standalone in nature, and implement local authorization decisions, without the ability to access networked infrastructure services that provide verification or status information. Another implication of this standalone environment is that it is infeasible to implement online key management mechanisms for establishing authentication keys between the PIV card and the secure site. Thus, physical access control systems tend to rely heavily upon offline or out-of-band means of pre-approving a cardholder for access to a particular secure site, and on the use of offline key management processes to obtain the site-specific authentication key that is injected into a PIV card to allow access to a particular secure site. As a result, physical access control systems are not typically able to support the scenario where a PIV cardholder can be authenticated in real-time to a secure site to which his access has not been pre-approved and pre-configured.

6.2.2 Applicable Authentication Mechanisms

Some PIV-supported authentication mechanisms for physical access control systems are described below.

Each of the authentication mechanisms described below can be further strengthened through the use of a backend certificate status verification infrastructure if the access control point has connectivity to the Agency's network infrastructure. Federal applications may augment authentication mechanisms for physical access control through the use of revocation status providers for the PIV card authentication certificate.

Table 6-1: Authentication Mechanisms for Physical Access

	Authentication Mechanism Steps	Comments
Visual Authentication	Guard inspects card for physical authenticity. Guard attempts to match facial characteristics of cardholder to picture on card. Identification information on card used for authorization check.	Human verification of card – may be rapid. Does not require backend infrastructure Low assurance mechanism since it is difficult to visually detect card forging and tampering. APPLICABLE IN ENVIRONMENTS THAT LACK CARD READERS
PACS Low Assurance Profile	Open read of PIV card to obtain the FASC-N and other data elements. FASC-N and other data elements used for authorization decision.	Rapid interaction with card. No change to PIV card for access to a new facility or resource. Does not require backend verification infrastructure. Minimal authentication assurance. Attacker can easily obtain FASC-N for an authorized person, and inject the FASC-N into a bogus PIV card. APPLICABLE WITH CONTACTLESS AND CONTACT-BASED CARD READERS.
PACS Medium Assurance Profile	Open read of PIV card to obtain the FASC-N and the Card Holder Unique Identifier (CHUID). Computation of an authentication string using the FASC-N and the Site Specific Key (SSK) for the site. Computed authentication string and other identification information on card used for authorization check.	Rapid interaction with card. No change to PIV card for access to a new facility or resource. Does not require backend verification infrastructure. Improved resistance to forgery. A bogus card injected with a valid FASC-N will be detected because it has a different CHUID. APPLICABLE WITH CONTACTLESS AND CONTACT-BASED CARD READERS.

	Authentication Mechanism Steps	Comments
Biometric Authentication	PIN is collected from the cardholder. PIN used to read biometric off the card. Biometric sample is collected from the cardholder and matched with value read from card. Open read of CHUID from card CHUID identifiers passed for authorization check.	Slower mechanism since it requires two interactions with the cardholder. No change to PIV card for access to a new facility or resource. Does not require backend verification infrastructure. Improved resistance to forgery, since biometric checked. Digital signature on biometric may be checked for higher assurance if control panel module has the capability to perform digital signature verification and if the latest certificate revocation information is accessible via some means. APPLICABLE WITH CONTACT-BASED CARD READERS.
PACS High Assurance Profile	Open read of CHUID from PIV card followed by a PACS-compliant challenge-response where the card responds using a site-specific authentication string (which was injected into the card in advance). A PIN is collected from the cardholder. Components of the CHUID, the PIN, and the SSK for that site is used in the computation to determine if response to challenge matches expected outcome.	Rapid interactions with card. Card has to be injected with site-specific authentication key that is used for challenge response interchange. Requires new authentication key injection for access to each new facility or resource. Does not require backend verification infrastructure. Rapid cryptographic computations on card. Highly resistant to forgery, unauthorized use, and Interposition type of threats. APPLICABLE WITH CONTACT-BASED CARD READERS.

6.3 Authentication for Logical Access Control

The PIV card may be used to authenticate the cardholder in support of access control decisions for information resources. For example, a cardholder may login to their agency network using the PIV card. The identity established through this authentication process can be used for determining access to file systems, databases, and other services available on the network.

6.3.1 Assumptions and Constraints

The logical access control environment is characterized by the following attributes:

- An untrusted network connects the PIV cardholder and the information resource.
- Logical access control points usually have sufficient network access to support the use of online key management schemes and online status lookups during the authentication process.
- Contact interface is preferred for logical access control.

Thus, typical logical access control systems are connected to networks of other systems and resources, have contact-based card readers, and have the ability to access networked infrastructure services that provide verification or status information. Logical access control environments can also support the implementation of online key management mechanisms for establishing authentication keys between the PIV card and the secure site.

6.3.2 Applicable Authentication Mechanisms

The Table 6-2 describes the authentication mechanisms defined for this standard for logical access control.

Table 6-2: Authentication Mechanisms for Logical Access

	Authentication Mechanism Steps	Comments
PKI Based challenge response	Challenge-response scheme between PIV card and card reader using the 1024 bit RSA PKI identity credential carried within the PIV card. Cardholder's PIN or biometric is used to authorize use of PKI identity credential (private key) held within PIV card. Relying party verifies the cardholder's certificate	No change to PIV card for access to a new facility or resource. Requires the availability of and access to backend certificate status checking infrastructure. Mechanism is resistant to forgery since digital credential is practically impossible to forge. Unauthorized use of PIV card is prevented through the use of an additional authentication factor (PIN and/or biometric) to authorize the use of

	Authentication Mechanism Steps	Comments
	chain and the response, and verifies the current revocation status of the certificate.	the authentication private key.

ANNEX A: PIV VALIDATION, CERTIFICATION, AND ACCREDITATION

HSPD-12 requires that all cards be issued by providers whose reliability is established by an official accreditation process. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. To help ensure reliability, agencies accredit issuers who issue identity credentials to their employees and contractors until a Government-wide PIV-II accreditation process is established. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system. NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" provides a formal framework for certification, along with specific requirements for validating and obtaining certificates for the PIV modules described below.

FIPS 201 provides security and interoperability requirements for PIV cards. NIST plans to develop a PIV Validation Program that will test implementations for conformance with this standard. Information on this program will be published at http://csrc.nist.gov/PIV-Project/Conformance/ as it becomes available.

The PIV system is FIPS 201 compliant after each of its constituent components (Card, Reader, Issuer Software and Registration Database) has met its individual validation requirements. Since these individual validation requirements are based on different standards and there is no single test laboratory that is accredited for validating products built to all of these standards, a PIV system has to undergo testing and consequent validation through multiple validation facilities. The PIV components and currently available validation requirements are summarized in Table A-1:

Table A-1: PIV System Components & Validation Requirements

PIV Component	Validation Requirement (s)
1. PIV ICC	(a) ISO/IEC 7816, ISO/IEC 10373 (Parts 1 and 3) (b) ISO/IEC 14443 (Parts 1-4), ISO/IEC 10373 (Part 6) (c) Crypto Modules – FIPS 140-2
2. PIV Reader	(a) PC/SC
3. Card Issuance and Management System	(a) Crypto Modules – FIPS 140-2

A.1 FIPS 140-2 Testing and Validation

All of the cryptographic modules in the PIV system (both on-card and issuer software) shall be FIPS 140-2 overall Level 2 (or higher) compliant. The test facilities for FIPS

140-2 testing (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) are the Cryptographic Module Testing (CMT) laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) program of the National Institute of Standards and Technology (NIST). Vendors wanting to supply cryptographic modules for the PIV system can select any of the accredited laboratories. The tests conducted by these laboratories for all vendor submissions are validated and a validation certificate for each vendor module is issued by the Cryptographic Module Validation Program (CMVP) – a joint program that is run by NIST and Communications Security Establishment (CSE), of Canada. The details of the CMVP, NVLAP programs and the list of CMT laboratories can be found in the CMVP website - http://csrc.ncsl.nist.gov/cryptval.

A.2 PIV System Validation, Certification and Accreditation Process

Assurance that PIV systems are compliant with FIPS 201 shall be provided through a comprehensive validation and NIST SP 800-37 certification and accreditation program (hereafter referred to as FIPS 201 Validation Program). FIPS 201 Validation, Certification and Accreditation program consists of:

a) Multiple Components: The FIPS 201 Validation program involves validation, certification and accreditation for an entire system (as opposed to a single product or module) that consists of multiple components.

b) Multiple Standards: Each of the PIV components may have to be validated for different standards.

The list of PIV components and the standards for which they must be validated are given in Table A-2 below:

Table A-2: PIV Components and Conforming Standard

PIV Component	Conforming Standard
1. PIV card – Physical Characteristics, Communication Protocol & Signals	(a) ISO/IEC 7810 (b) ISO/IEC 7816 (c) ISO/IEC 14443
2. PIV card – ON-card Crypto Modules & associated Algorithms	FIPS 140-2
3. PIV Reader	(a) PC/SC
4. Card Issuance and Management System	FIPS 140-2

A.2.1 Scope of FIPS 201 Validation Testing

The FIPS 201 Validation program will not involve testing for compliance to every one of the standards referred above. PIV components conforming to industry-wide standards are procured pre-validated. The following pre- validated PIV components will not be subject to unit tests under the FIPS 201 Validation program.

Table A-3: Standards for Pre-validated Components

Pre-Certified PIV Component	Associated Standard
1. PIV card (without Crypto Modules)	ISO IEC 7816, ISO/IEC 14443
2. PIV Reader	PC/SC

The following PIV components shall be subject to validation under the FIPS 201 Validation Program. The rationale for choosing these components for direct testing is that they are either function modules involved in the core function of identity credential verification or service modules called from those function modules to perform specific functions (e.g., crypto-service modules performing functions like signing a message, verifying a message signature, retrieving a certificate etc).

Table A-4: Standards for Validated Components

FIPS 201 Validated PIV Component	Associated Standard
1. PIV card –On-card Crypto Modules	FIPS 140-2
2. Card Issuance and Management System	FIPS 140-2

The FIPS 140-2 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) standard stipulates certain security requirements for cryptographic modules (both hardware and software and firmware) and categorizes those requirements into four overall levels in the increasing order of stringency. At a minimum, the crypto module used in a PIV component (on-card or in issuer software) shall be validated at FIPS 140-2 overall Level 2. In addition, PIV cards shall be validated at Level 3 for Physical Security and Operator Authentication.

Besides conformance to the established standards, FIPS 201 validation may involve some minor tests for conformance to the issuing agency's policies, such as the verification of the credentials in the PIV card for conformance to the issuing agency's privacy policy.

Since the FIPS 201 card is intended to provide, not only physical access, but also logical access to IT systems, a FIPS 201 card shall include modules that support access control/authorizations by a variety of information systems supported by issuing agencies. These modules, irrespective of whether they are resident in the PIV card or in the issuer software (client application), will not come directly under the scope of FIPS 201 validation testing, but will be part of the NIST SP 800-37 certification and accreditation process.

A.2.2 Tasks for Setting up the FIPS 201 Validation Program

The following tasks shall be undertaken by NIST to set up the FIPS 201 Validation Program.

a) Accreditation of Testing Laboratories — Testing Laboratories involved in FIPS 201 testing will be accredited through the National Voluntary Laboratory

Accreditation Program (NVLAP). Since there already exist laboratories (i.e., the Cryptographic Module Testing (CMT) laboratories) for FIPS 140-2 testing under this accreditation scheme, the main task will be to accredit laboratories for FIPS 201 testing.

b) Guidance Documents — NIST shall develop guidance documents for various stakeholders. This shall include PIV component vendors who want to have their products validated for FIPS 201

A.2.3 Steps for Acquiring FIPS 201 Validation, Certification, and Accreditation

a) Vendors interested in having their products validated for FIPS 201 compliance may approach any of the FIPS 201 accredited laboratories for testing their PIV system modules.

b) The accredited laboratories shall perform the tests conforming to the relevant standards specified in FIPS 201.

c) The tests shall be validated and a certificate will be issued by the FIPS 201 Validation Program office for those modules that were tested.

d) The information system must be certified and accredited in accordance with the guidelines contained in NIST SP 800-37.

A.2.4 Validation Maintenance

It is anticipated that there will be activities performed on one or more of the PIV system modules by the issuing agency after the procurement of a FIPS 201 validated product and issuance of PIV cards. Examples of these post-issuance activities include:

a) New applications are loaded to the PIV card by another agency.

b) Application modified for access to new information systems or changing access control mechanisms for existing PIV system.

These two types of post-issuance activities have different impacts on FIPS 201 validation. Whenever there is a change in the card issuance system and card design, the issuing agency shall re-validate the PIV card issuance system to ensure that privacy requirements are still met. Whenever new modules are added to the card or the issuer software, re-validation shall be required in order to ensure that these new modules do not interfere with the crypto modules or affect the interoperability between the issuer software and the PIV card.

A.2.5 Internal Auditing for PIV card Management

To detect issuance of fraudulent cards or other malfeasance by the personnel operating the PIV card system, implementing agencies shall rely upon regular audit reviews conducted by a trusted third party in addition to implementing the NIST SP 800-37 certification and accreditation process. The PIV system auditor may not hold any other operational role in the system.

ANNEX B: ACCESS CONTROL MECHANISMS (INFORMATIVE)

FIPS 201 provides identity card-based support for both logical and physical access control systems.

B.1 Physical Security Support

The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group has drafted *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* (PACS). Table B-1 differentiates among low, moderate, and high PACS assurance profiles and lists PIV card features available to support the three profiles.

Table B-1: PIV Support for PACS

Assurance Level	Basic Requirement	PIV card Support
PACS Low	Recognition of Unique Cardholder Identifier string (i.e., FASC-N) and matching to Access List	Unique Cardholder Identifier string (i.e., FASC-N)
PACS Medium	Use of Unique Cardholder Identifier string (i.e., FASC-N) and Card Unique Identifier (i.e., CUID) to derive unique authentication string and matching to access list.	Unique Cardholder Identifier string (i.e., FASC-N) and Card Unique Identifier (i.e., CUID). Digitally Signed Unique Card Identifier and Expiration Date[7]
PACS High	Cryptographic Challenge/Response Protocol	PIN Capture/Storage and Cryptographic Engine and Key Management Support
Other Support Features	-	Signed Digital Biometric Information That Can Be Used In Matching of Biometric Information Stored on Card to Biometric Information Captured By Access Control Mechanisms

[7] *The PIV standard extends the standard CHUID data structure to add a Expiration Date element as described in Section 4.2.1.*

B.2 Logical Access Support

For logical access control, FIPS 201 incorporates by reference [NIST800-63] [NIST800-3] supplements OMB guidance, *E-Authentication Guidance for Federal Agencies* (OMB 04-04) that defines four levels of authentication Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance, and Level 4 is the highest. Table B-2 summarizes electronic authentication requirements and PIV support to electronic authentication functions.

Table B-2: PIV Support for E-Authentication

Assurance Level	Basic Requirement	PIV card Support
1	Password-based Access Control	
2	Access control Based on “Strong Passwords”	
3	Proof of Possession of a Key or a One-time Password Through a Cryptographic Protocol.	Cryptographic Mechanisms Including Signed Key Certificate (May use “soft” Card or one-time password device)
4	-	Cryptographic Mechanisms Including Signed Key Certificate (Must use “hard” Card)

ANNEX C: BIOMETRIC ENROLLMENT CHECKS

This Annex presents the descriptors and field specifications for type-14 logical records used with flats based civil background checks. The flat fingerprint impressions are contained in three type-14 image records. Two of the image records contain the left and right simultaneous four fingers, and the third contains the two thumbs. Offsets to the locations of image segments containing the individual fingers are included with the image records. Most of the following definitions are taken from the ANSI Standard, Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information (ANSI/NIST-ITL 1-2000).

- BPX 14.012 - BITS PER PIXEL. This mandatory ASCII field shall contain the number of bits used to represent a pixel. This field shall contain an entry of .8. for normal grayscale values of .0. to .255.

- CGA 14.011 - COMPRESSION ALGORITHM. This mandatory ASCII field shall specify the algorithm used to compress grayscale images. An entry of "NONE" in this field indicates that the data contained in this record is uncompressed. For those images that are to be compressed, this field shall contain “WSQ”the preferred method for the compression of tenprint fingerprint images.

- COM 14.020 - COMMENT. This optional field may be used to insert comments or other ASCII text information with the tenprint image data.

- DAT 14.999 - IMAGE DATA. This field shall contain all of the data from a captured tenprint image. It shall always be assigned field number 999 and must be the last physical field in the record. For example, .14.999:. is followed by image data in a binary representation. Each pixel of uncompressed grayscale data shall be quantized to eight bits (256 gray levels) contained in a single byte. If compression is used, the pixel data shall be compressed in accordance with the compression technique specified in the CGA field.

- FGP 14.013 – FINGER POSITION. This mandatory tagged-field shall contain finger position code that matches the tenprint image. The decimal code number corresponding to the known or most probable finger position shall be taken from Table 1 and entered as a one or two character ASCII subfield. Table 1 also lists the maximum image area that can be transmitted for each of the fourteen possible finger positions.

Table C-1: Finger Position Code and Maximum Size

Finger Position	Finger Code	Width		Length	
		(mm)	(in)	(mm)	(in)
Unknown	0	40.6	1.6	38.1	1.5
Right thumb	1	40.6	1.6	38.1	1.5
Right index finger	2	40.6	1.6	38.1	1.5
Right middle finger	3	40.6	1.6	38.1	1.5
Right ring finger	4	40.6	1.6	38.1	1.5
Right little finger	5	40.6	1.6	38.1	1.5
Left thumb	6	40.6	1.6	38.1	1.5
Left index finger	7	40.6	1.6	38.1	1.5
Left middle finger	8	40.6	1.6	38.1	1.5
Left ring finger	9	40.6	1.6	38.1	1.5
Left little finger	10	40.6	1.6	38.1	1.5
Plain right thumb	11	25.4	1.0	50.8	2.0
Plain left thumb	12	25.4	1.0	50.8	2.0
Plain right four fingers	13	83.8	3.3	76.2	3.0
Plain left four fingers	14	83.8	3.3	76.2	3.0
Left and Right thumbs	15	50.8	2.0	76.2	3.0

- HLL 14.006 - HORIZONTAL LINE LENGTH. This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image.

- HPS 14.009 - HORIZONTAL PIXEL SCALE. This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the horizontal component of the pixel aspect ratio.

- IDC 14.002 - IMAGE DESIGNATION CHARACTER. This mandatory ASCII field shall be used to identify the tenprint fingerprint image contained in the record. This IDC shall match the IDC found in the file content (CNT) field of the Type-1 record.

- IMP 14.003 - IMPRESSION TYPE. This mandatory one-byte ASCII field shall indicate the manner by which the tenprint mage information was obtained. The appropriate code selected from Table 2 shall be entered in this field.

- IQM 14.022 – IMAGE QUALITY METRIC. This mandatory ASCII field shall contain the image quality scores for the individual fingers. Each finger score is defined by the FINGER NUMBER and the QUALITY SCORE separated by the <US> separator. Individual finger quality definitions are separated by the <RS> separator.

Table C-2 - Finger Impression Type

Description	Code
Live-scan plain	0
Live-scan rolled	1
Nonlive-scan plain	2
Nonlive-scan rolled	3
Latent impression	4
Latent tracing	5
Latent photo	6
Latent lift	7

- LEN 14.001 - LOGICAL RECORD LENGTH. This mandatory ASCII field shall contain the total count of the number of bytes in the Type-14 logical record. Field 14.001 shall specify the length of the record including every character of every field contained in the record and the information separators.

- SEG 14.021 – FINGER SEGMENT POSITION(s). This mandatory ASCII field shall contain offsets to the locations of image segments containing the individual fingers within the image. The offsets are relative to the origin, (0,0), which is in the upper left corner of the image. The horizontal offsets (X) are the pixel counts to the right, and the vertical offsets (Y) are the pixel counts down. A finger segment is defined by the FINGER NUMBER, the X coordinates (LEFT , RIGHT) and the Y coordinates (TOP, BOTTOM), of its bounding box. The five information items within a finger segment definition are separated by the <US> separator. Individual finger segment definitions are separated by the <RS> separator.

- SLC 14.008 - SCALE UNITS. This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A "1" in this field indicates pixels per inch, or a 2" indicates pixels per centimeter. A "0" in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

- SRC 14.004 - SOURCE AGENCY. This mandatory ASCII field shall contain the identification of the administration or organization that originally captured the tenprint image contained in the record. Normally, the ORI of the agency that captured the image will be contained in this field. The SRC may contain up to 20 identifying characters and the data content of this field shall be defined by the user and be in accordance with the receiving agency.

- TCD 14.005 - TENPRINT CAPUTRE DATA. This mandatory ASCII field shall contain the date that the tenprint image was captured. The date shall appear as eight digits in the format CCYYMMDD. The CCYY characters shall represent the year the image was captured; the MM characters shall be the tens and units values of the month; and the DD characters shall be the tens and units values of the day in the month. For example, the entry 20000229 represents February 29, 2000. The complete date must be a legitimate date.

- VLL 14.007 - VERTICAL LINE LENGTH. This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image.

- VPS 14.010 - VERTICAL PIXEL SCALE. This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the vertical component of the pixel aspect ratio.

ANNEX D: BACKGROUND CHECK REQUIREMENTS

The NAC, NACI, NACIC, LBI, and BI are defines as follows:

NAC — The NAC is a part of every NACI, NACIC, LBI, and BI. Standard NACs are: Security/Suitability Investigations Index (SII), Defense Clearance Investigation Index (DCII), FBI Name Check, FBI National Criminal History Fingerprint check.

NACI — The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes:

- Employment 5 years
- Education 5 years and highest degree verified
- Residence 3 years
- References
- Law Enforcement 5 years
- NACs

NACIC – This NACI includes the addition of a credit record search.

LBI – This investigation includes a NACIC, personal subject interview, and personal interviews by an investigator of subject's background during the most recent three years. Coverage includes:

- PRSI Personal Subject Interview
- Employment 3 years
- Education 3 years and highest degree verified
- Residence 1 year
- References 1 year
- Law Enforcement 5 years
- Court Records 3 years
- Credit 7 years
- NACs

BI – This is a more in-depth version of the LBI since the personal investigation coverage is the most recent five to seven years. This investigation is required of those going into “high risk” public trust positions. Coverage includes:

- PRSI Personal Subject Interview
- Employment 5 years
- Education 5 years and highest degree verified
- Residence 3 years
- Law Enforcement 5 years
- Court Records 5 years
- Credit 7 years

ANNEX E: GLOSSARY OF TERMS AND ACRONYMS

E.1 Glossary of Terms

The following definitions are used throughout this standard:

Application: A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate the end user's interaction with the system.

Access control: The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

Applicant: An individual requesting a PIV credential. The applicant may be a new Federal hire, Federal employee or contractor.

Approved: FIPS approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.

Architecture: A highly structured specification of an acceptable approach within a framework for solving a specific problem and containing descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable in order to satisfy related constraints (e.g., costs, local environment, user acceptability).

Asymmetric keys: Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Authentication: The process of establishing confidence in user identities.

Biometric: A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples of biometrics.

Biometric Information: The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g. patterns.)

Biometric System: An automated system capable of:

- capturing a biometric sample from an end user;
- extracting biometric data from that sample;
- comparing the biometric data with that contained in one or more reference templates;
- deciding how well they match; and
- indicating whether or not an identification or verification of identity has been achieved.

Biometric Template: A characteristic of a biometric information (e.g. minutiae or patterns.)

Cardholder: An individual possessing an issued PIV card.

Capture: The method of taking a biometric sample from an end user. [INCITS/M1-040211]

Certificate Revocation List: A list of revoked public key certificates created and digitally signed by a Certification Authority. [RFC 3280]

Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.

Certification Authority: A trusted entity that issues and revokes public key certificates.

Credential: An object that authoritatively binds an identity (and optionally, additional attributes) to and are controlled by an individual.

Comparison: The process of comparing a biometric with a previously stored reference template or templates. See also 'One-To-Many' and 'One-To-One' [INCITS/M1-040211]

Claimant: A party whose identity is to be verified using an authentication protocol.

Component: An element of a large system in general; specifically, an identity card, issuing authority, registration authority, Card reader, and identity verification support etc. within the personal identity verification system.

Conformance testing: a process established by NIST within its responsibilities of developing, promulgating, and supporting Federal Information Processing Standards for testing specific characteristics of components, products, and services as well as people and organizations for compliance with a FIPS standard.

Cryptographic key (key): A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

False acceptance: When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity. [INCITS/M1-040211]

False Acceptance Rate/FAR: The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The False Accept Rate may be estimated as follows:
FAR = NFA / NIVA
where
FAR is the false acceptance rate
NFA is the number of false acceptances
NIVA is the number of impostor verification attempts
[INCITS/M1-040211]

False Match Rate/FMR: Alternative to 'False Acceptance Rate'. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an applicant. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of

'False Acceptance' and 'False Rejection'. See also 'False Non-Match Rate'. [INCITS/M1-040211]

False Non Match Rate/FNMR: Alternative to 'False Rejection Rate'. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an applicant. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'. See also 'False Match Rate'. [INCITS/M1-040211]

False rejection: When a biometric system fails to identify an applicant or fails to verify the legitimate claimed identity of an applicant. [INCITS/M1-040211]

False Rejection Rate/FRR: The probability that a biometric system will fail to identify an applicant, or verify the legitimate claimed identity of an applicant. The False Rejection Rate may be estimated as follows:
FRR = NFR / NEVA
where
FRR is the false rejection rate
NFR is the number of false rejections
NEVA is the number of applicant verification attempts
This estimate assumes that the applicant verification attempts are representative of those for the whole population of end-users. The False Rejection Rate normally excludes 'Failure to Acquire' errors. [INCITS/M1-040211]

Federal Information Processing Standard (FIPS): A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Graduated security: A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.

Hash based message authentication code (HMAC): A message authentication code that uses a cryptographic key in conjunction with a hash function.

Hash function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

1. (One-way) - It is computationally infeasible to find any input that maps to any pre-specified output, and
2. (Collision resistant) - It is computationally infeasible to find any two distinct inputs that map to the same output.

HMAC: See Hash based message authentication code.

Identifier: A unique data string used as a key in the biometric system to name a person's *identity* and its associated attributes. An example of an *identifier* would be a Card number.

Identity: A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.

.

Identification: The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Identity proofing: The process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV Registration Authority when attempting to establish an identity.

Identity registration: The process of making a person's *identity* known to the PIV system, associating a unique *identifier* with that identity, and collecting and recording the person's relevant attributes into the system.

Identity verification: The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity card or PIV system.

Interoperability: For the purposes of this standard, interoperability allows any Government facility or information system, regardless of the cardholder's parent organization, to authenticate cardholder's identity using the credentials stored on the PIV card.

Issuer: See parent organization.

JPEG: A standardized image compression function originally established by the Joint Photographic Experts Group.

Key: See cryptographic key.

Match/matching: The process of comparing biometric information against a previously stored template(s) and scoring the level of similarity.

Mandatory Topography: See Standard Topography.

Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.

Model: A very detailed description or scaled representation of one component of a larger system that may be created, operated, and analyzed to predict actual operational characteristics of the final produced component.

Off-card: Refers to data that is not stored within the PIV card or computation that is not done by the ICC of the PIV card.

On-card: Refers to data that is stored within the PIV card or computation that is done by the ICC of the PIV card.

One-to-many: Synonym for 'Identification' [INCITS/M1-040211]

One-to-one: Synonym for 'Verification' [INCITS/M1-040211]

Online Certification Status Protocol (OCSP): An on-line protocol used to determine the status of a public key certificate. [RFC 2560]

Optional Topography*:* A topography that contains both the mandatory and optional topographical features of this standard.

Personal identification number (PIN): A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.

Parent Organization: The organization that is applying for the PIV card on behalf of an applicant. Typically this is an organization for whom the applicant is working.

Personal Identity Verification (PIV) Card: Physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

PIV Requesting Official: An individual who can act on behalf of an agency to request a credential for an applicant.

PIV Authorizing Official: An individual who can act on behalf of an agency to authorize the issuance of a credential to an applicant.

*PIV Issuance Authority: A*n authorized identity card creator that procures FIPS approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the card with the identity credentials of the authorized subject, and delivers the personalized card to the authorized subject along with appropriate instructions for protection and use.

PIV Registration Authority: An entity that establishes and vouches for the identity of an applicant to a PIV Issuing Authority. The PIV RA authenticates the applicant's identity by checking identity source documents and identity proofing and ensures a proper background check has been completed before the credential is issued.

Population: The set of end-users for the application. [INCITS/M1-040211]

Position Sensitivity Levels: The four OPM-specified sensitivity levels assigned to a particular job or position. See *Sensitivity Levels.*

Public Key: The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key Infrastructure (PKI): A support service to the PIV system that provides cryptographic keys needed to verify digital signature based identity verification and to protect

communications and storage of sensitive verification system data within identity Cards and the verification system.

Registration: See Identity Registration

Recommendation: A special publication of the Information Technology Laboratory stipulating specific characteristics of technology to use or procedures to follow in order to achieve a common level of quality or level of interoperability.

Secret key: A cryptographic key that must be protected from unauthorized disclosure in order to protect data encrypted with the key. The use of the term "secret" in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.

Sensitivity levels: A graduated system of marking (e.g., low, moderate, high) information and information processing systems based on threats and risks that result if a threat is successfully conducted.

Standard: A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard.

Template: A biometric image data record. [INCITS/M1-040211]

Topography: The physical, non-logical features of a card. A card may have either standard or enhanced topography.

Validation: The process of demonstrating that the system under consideration meets in all respects the specification of that system. [INCITS/M1-040211]

Verification: See Identity Verification.

E.2 Acronyms

The following acronyms and abbreviations are used throughout this standard:

AID Application Identifier

AIM Association for Automatic Identification and Mobility

ANSI American National Standards Institute

ATR Answer-to-Reset

CA Certificate Authority

CAD Card Accepting Device

CHUID Cardholder Unique Identification

CRL	Certificate Revocation List
EFTS/F	Electronic Fingerprint Transmission Specification
FASC-N	Federal Agency Smart Credential Number
FID	File ID
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
GSC	Government Smart Card
HSPD	Homeland Security Presidential Directive
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NFIQ	NIST Fingerprint Image Quality
OCSP	On-line Certificate Status Protocol
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
RFU	Reserved for Future Use
ST	Status Tuple
TLV	Tag-Length-Value
WSQ	Wavelet Scalar Quantization

ANNEX F: REFERENCES

[ANSI322] ANSI INCITS 322 Information Technology, Card Durability Test Methods, ANSI, 2002.

[CBEFF] NISTIR 6529-A - Common Biometric Exchange Formats Framework (CBEFF), NIST Interagency Report, 2003.

[COMMON] X.509 Certificate Policy for the Common Policy Framework, February 10, 2004. Available at http://www.cio.gov/ficc/documents/CommonPolicy.pdf.

[FIBIF] ANSI/INCITS 381-2004 - Finger Image Based Interchange Format, ANSI, 2004.

[FFSMT] ANSI/NIST-ITL 1-2000 – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, ANSI, 2000.

[EFTS/F] Appendix F of the FBI's Electronic Fingerprint Transmission Specification (EFTS/F), EFTS70, Department of Justice, Federal Bureau of Investigation, January, 1999.

[FLATS] NISTIR 7110 - C. L. Wilson, M. D. Garris, and C. I. Watson, Matching Performance for the USVISIT IDENT System Using Flat Fingerprints, National Institute of Standards and Technology, (May 2004).

[FRFD] ANSI/INCITS 385-2004 - Face Recognition Format for Data Interchange, ANSI, May 2004.

[G90-98] ASTM G90-98 – Standard Practice for Performing Accelerated Outdoor Weathering of Non-metallic Materials Using Concentrated Natural Sunlight, ASTM, Vol. 14.04, 2003.

[G155-00] ASTM G155-00 – Standard Practice for Operating Xenon Arc Light Apparatus for Exposure of Non-metallic Materials, ASTM, Vol. 14.04, July 2000.

[GP] GlobalPlatform, Open Platform Card Specification, Version 2.0.1, April 7, 2000.

[INCITS/M1-040211] ANSI/INCITS M1-040211 – Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers, ANSI, April 2004.

[IR7116] NISTIR 7116, Time Synchronization for Electronic Distributed Systems, NIST, May 2004.

[ISO14443] ISO/IEC 14443-1:2000 Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards, 2000-04-15, ISO, 2000.

[ISO10373] ISO/IEC 10373, Identification cards – Test methods. Part 1 – Standard for General Characteristic Test of Identification Cards, ISO, 1998. Part 3 – Standard for Integrated Circuit Cards with Contacts and Related Interface Devices, ISO, 2001. Part 6 – Standard for Proximity Card Support in Identification Cards, ISO, 2001.

[ISO7810] ISO/IEC 7810:2003 Identification Cards – Physical Characteristics, 2003-11-01, ISO, 2003.

[ISO7816] ISO/IEC 7816, Parts 1-6, Identification Cards – Integrated Circuits with Contacts http://www.iso.ch.

[MINEX04] – Minutiae Interoperability Exchange Test 2004, http://fingerprint.nist.gov/minex04/index.html, NIST, 2004.

[NFIQUA] NISTIR 7151 – NIST Fingerprint Image Quality (NFIQ), NIST, August 2004.

[OMB130] Management of Federal Information Resources, Office of Management and Budget, OMB A-130, February 1996.

[OMBx04] Office of Management and Budget, OMB 04-04, December 2003.

[PACS] PACS v2.2 – The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2 July 27, 2004.

[PCSC] – Personal Computer/Smart Card Workgroup Specifications, http://www.pcscworkgroup.com.

[PDF417] Uniform Symbology Specification – PDF417, Association for Automatic Identification and Mobility (AIM), August 1994.

[PROF] X.509 Certificate and CRL Profile for the Common Policy, Version 1.1 July 8, 2004. Available at http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf

[SP8x30] Risk Management Guide for Information Technology System, NIST Special Publication 800-30, NIST, July 2002.

[SP8x37] Guide for Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, NIST, May 2004.

[SP8x53] Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, NIST, September 2004 (2PD).

[SP800-63] Appendix A in NIST SP 800-63, *Electronic Authentication Guideline*: Recommendations of the National Institute of Standards and Technology, NIST, June 2004.

[SP800-73] Integrated Circuit Card for Personal Identity Verification, Special Publication 800-73, Version 1.0, NIST, 2004-10-19.

[SSP REP] Shared Service Provider Repository Service Requirements, January 23, 2004. Available at http://www.cio.gov/ficc/documents/SSPrepositoryRqmts.pdf

[VEND1] NIST IR 6965 - P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and M. Bone, ‘Face recognition vendor test 2002, National Institute of Standards & Technology, Gaithersburg Maryland, March 2003.

[VEND2] NISTIR 7123 - C.L. Wilson, R. Austin Hicklin, Harold Korves, Bradford Ulery, Melissa Zoepfl, Mike Bone, Patrick Grother, Ross Micheals. Steve Otto and, Craig Watson, Fingerprint vendor technology evaluation 2003: summary of results and analysis report, National Institute of Standards and Technology, (June 2004).